vSphere Upgrade

Update 2
vSphere 5.5

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-001516-00

vmware®

You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About vSphere Upgrade

vSphere Upgrade describes how to upgrade VMware vSphere™ to the current version.

To move to the current version of vSphere by performing a fresh installation that does not preserve existing configurations, see the *vSphere Installation and Setup* documentation.

Intended Audience

vSphere Upgrade is for anyone who needs to upgrade from earlier versions of vSphere. These topics are for experienced Microsoft Windows or Linux system administrators who are familiar with virtual machine technology and data center operations.

Overview of the Upgrade Process 1

Upgrading is a multistage process in which procedures must be performed in a particular order. Follow the process outlined in this high-level overview to ensure a smooth upgrade with a minimum of system downtime.

IMPORTANT Make sure that you understand the entire upgrade process before you attempt to upgrade. If you do not follow the safeguards, you might lose data and access to your servers. Without planning, you might incur more downtime than is necessary.

If you use vCenter Server Heartbeat in your vSphere deployment, use the *vSphere Server Heartbeat* installation and upgrade documentation to upgrade vCenter Server.

vCenter Server 5.5 removes support for Windows Server 2003 as a host operating system. See the VMware Compatibility Guide at http://www.vmware.com/resources/compatibility/search.php and "Migrate vCenter Server and Components from a Windows Server 2003 Host," on page 109.

vCenter Server 5.5 removes support for Windows Server 2008 SP1 as a host operating system. Upgrade Windows Server 2008 SP1 hosts to SP2 before upgrading vCenter Server to version 5.5. See the VMware Compatibility Guide at http://www.vmware.com/resources/compatibility/search.php and the Microsoft Software Lifecycle Policy at http://support.microsoft.com/lifecycle/#ServicePackSupport.

You must complete the upgrade process in a specific order because you can lose data and server access. Order is also important within each upgrade stage.

You can perform the upgrade process for each component in only one direction. For example, after you upgrade to vCenter Server 5.x, you cannot revert to vCenter Server 4.x. With backups and planning, you can restore your original software records.

You must complete one procedure before you move to the next procedure. Follow the directions within each procedure regarding the required sequence of minor substeps.

Because certain commands can simultaneously upgrade more than one stage, VMware recommends that you understand the irreversible changes at each stage before you upgrade your production environments.

To ensure that your datacenter upgrade goes smoothly, you can use vCenter Update Manager to manage the process for you.

vSphere upgrades proceed in the following sequence of tasks.

1. If your vSphere system includes VMware solutions or plug-ins, make sure they are compatible with the vCenter Server version that you are upgrading to. See the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.
2. If you are upgrading vSphere components that are part of a VMware View environment, see "Upgrading vSphere Components Separately in a Horizon View Environment," on page 220.

3 Make sure your system meets vSphere hardware and software requirements.

   See Chapter 2, "System Requirements," on page 13.

4 Upgrade vCenter Single Sign-On, vCenter Inventory Service, vCenter Server, and the vSphere Web Client.

   IMPORTANT If you use vCenter Server Heartbeat in your vSphere deployment, use the *vSphere Server Heartbeat*installation and upgrade documentation to upgrade vCenter Server and related components.

   See Chapter 4, "Upgrading vCenter Server," on page 61. Use the topic "Required Information for Installing or Upgrading vCenter Single Sign-On, Inventory Service, vCenter Server, and the vSphere Web Client," on page 41 to create a worksheet with the information you will need when you install vCenter Single Sign-On, vCenter Inventory Service, and vCenter Server.

5 If you use VMware Update Manager, upgrade VMware Update Manager.

   See Chapter 6, "Upgrading Update Manager," on page 139.

6 Upgrade your ESXi hosts.

   See Chapter 7, "Upgrading and Migrating Your Hosts," on page 143. vSphere provides several ways to upgrade hosts:

   - Use vSphere Update Manager to perform an orchestrated upgrade of your ESXi hosts. See "Using vSphere Update Manager to Perform Orchestrated Host Upgrades," on page 166.
   - Upgrade a single host at a time, interactively, from an ESXi ISO installer image stored on a CD, DVD, or USB flash drive. See "Upgrade or Migrate Hosts Interactively," on page 180.
   - Use a script to perform an unattended upgrade for multiple hosts. See "Installing, Upgrading, or Migrating Hosts Using a Script," on page 182
   - If a host was deployed using vSphere Auto Deploy, you can use Auto Deploy to upgrade the host by reprovisioning it. See "Using vSphere Auto Deploy to Reprovision Hosts," on page 196.
   - Upgrade or patch ESXi 5.x hosts by using `esxcli` commands. See "Upgrading Hosts by Using esxcli Commands," on page 200.

7 Reapply your host license.

   See "Reapplying Licenses After Upgrading to ESXi 5.5," on page 214.

8 Upgrade virtual machines and virtual appliances, manually or by using VMware Update Manager to perform an orchestrated upgrade.

   See Chapter 8, "Upgrading Virtual Machines and VMware Tools," on page 215.

This chapter includes the following topics:

How vSphere 5.x Differs from vSphere 4.x

vSphere 5.x is a major upgrade from vSphere 4.x.

The following changes from vSphere 4.x affect vSphere installation and setup. For a complete list of new features in vSphere 5.x, see the release notes for version 5.x releases.

Service Console is removed

ESXi does not include a Service Console. You can perform most tasks that you performed in the Service Console by using esxcli commands in the ESXi Shell, by using vCLI commands, and by using VMware PowerCLI commands. See *Command-Line Management in vSphere 5.0 for Service Console Users* and *Getting Started with vSphere Command-Line Interfaces*.

ESXi does not have a graphical installer

The graphical installer relied on the Service Console, which is not a part of ESXi. ESXi retains the text-based installer.

vSphere Auto Deploy and vSphere ESXi Image Builder CLI

Before ESXi 5.0, ESXi was installed on the physical disk of each ESXi host. With ESXi 5.x, you can load an ESXi image directly into memory by using vSphere Auto Deploy. You can provision and reprovision large numbers of ESXi hosts efficiently with vCenter Server, and manage ESXi updates and patching by using an image profile. You can save host configuration such as network or storage setup as a host profile and apply it to the host by using Auto Deploy. You can use ESXi Image Builder CLI to create ESXi installation images with a customized set of updates, patches, and drivers.

For complete information on using vSphere Auto Deploy and ESXi Image Builder PowerCLI, see the *vSphere Installation and Setup* documentation.

Changes in the ESXi installation and upgrade process

ESXi 5.x uses a single installer wizard for fresh installations and upgrades. ESXi 5.x also provides a new option for deploying ESXi directly into the host memory with vSphere Auto Deploy. The `vihostupdate` and `esxupdate` utilities are not supported for ESXi 5.x. You cannot upgrade or migrate from earlier ESX or ESXi versions to ESXi 5.x by using any command-line utility. After you have upgraded or migrated to ESXi 5.x, you can upgrade or patch ESXi 5.x hosts using vCLI `esxcli` commands.

IMPORTANT After you upgrade or migrate your host to ESXi 5.x, you cannot roll back to your version 4.x ESX or ESXi software. Back up your host before you perform an upgrade or migration, so that, if the upgrade or migration fails, you can restore your 4.x host.

See "ESXi 5.5 Upgrade Options," on page 150.

Installer caching

Instead of using a binary image to install the system, whatever bits were used at boot time are cached to the system. This caching reduces installation problems caused by accessing installation files across networks that are under load.

NOTE Scripted installations cannot PXE boot a server and then obtain the binary image from some other form of media.

Changes to partitioning of host disks

All freshly installed hosts in vSphere 5.x use the GUID Partition Table format instead of the MSDOS-style partition label. This change supports ESXi installation on disks larger than 2TB.

Newly installed vSphere 5.x hosts use VMFS5, an updated version of the VMware File System for vSphere 5.x. Unlike earlier versions, ESXi 5.x does not create VMFS partitions in second and successive disks.

Upgraded systems do not use GUID Partition Tables (GPT), but retain the older MSDOS-based partition label.

VMware vCenter Server Appliance

As an alternative to installing vCenter Server on a Windows machine, vSphere 5.x provides the VMware vCenter Server Appliance. The vCenter Server Appliance is a preconfigured Linux-based virtual machine optimized for running vCenter Server and associated services.

vSphere Web Client

The vSphere Web Client is a server application that provides a browser-based alternative to the deprecated vSphere Client. You can use a Web browser to connect to the vSphere Web Client to manage an ESXi host through a vCenter Server.

vCenter Single Sign-On

vSphere versions 5.1 and later include vCenter Single Sign-On as part of the vCenter Server management infrastructure. This change affects vCenter Server installation, upgrading, and operation. Authentication by vCenter Single Sign-On makes the VMware cloud infrastructure platform more secure by allowing the vSphere software components to communicate with each other through a secure token exchange mechanism, instead of requiring each component to authenticate a user separately with a directory service like Active Directory. See "How vCenter Single Sign-On Affects vCenter Server Upgrades," on page 32

Differences Between vSphere Upgrades and Updates

vSphere products distinguish between upgrades, which make major changes to the software, and updates, which make smaller changes to the software.

VMware product versions are numbered with two digits, for example, vSphere 5.1. A release that changes either digit, for example, from 4.1 to 5.0, or from 5.0 to 5.1, involves major changes in the software, and requires an upgrade from the previous version. A release that makes a smaller change, requiring only an update, is indicated by an update number, for example, vSphere 5.1 Update 1.

When you upgrade an ESXi host, some host configuration information is preserved in the upgraded version, and the upgraded host, after rebooting, can join a vCenter Server instance that has been upgraded to the same level. Because updates and patches do not involve major changes to the software, host configuration is not affected.

System Requirements 2

Systems running vCenter Server and ESXi instances must meet specific hardware and operating system requirements.

If you are using Auto Deploy to provision ESXi hosts, see also the information about preparing for VMware Auto Deploy in the *vSphere Installation and Setup* documentation.

This chapter includes the following topics:

ESXi Hardware Requirements

Make sure the host meets the minimum hardware configurations supported by ESXi 5.5.

Hardware and System Resources

To install and use ESXi 5.5, your hardware and system resources must meet the following requirements:

- Supported server platform. For a list of supported platforms, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility.
- ESXi 5.5 will install and run only on servers with 64-bit x86 CPUs.
- ESXi 5.5 requires a host machine with at least two cores.
- ESXi 5.5 supports only LAHF and SAHF CPU instructions.
- ESXi 5.5 requires the NX/XD bit to be enabled for the CPU in the BIOS.

- ESXi supports a broad range of x64 multicore processors. For a complete list of supported processors, see the VMware compatibility guide at http://www.vmware.com/resources/compatibility.
- ESXi requires a minimum of 4GB of physical RAM. Provide at least 8GB of RAM to take full advantage of ESXi features and run virtual machines in typical production environments.
- To support 64-bit virtual machines, support for hardware virtualization (Intel VT-x or AMD RVI) must be enabled on x64 CPUs.
- One or more Gigabit or 10Gb Ethernet controllers. For a list of supported network adapter models, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility.
- Any combination of one or more of the following controllers:
  - Basic SCSI controllers. Adaptec Ultra-160 or Ultra-320, LSI Logic Fusion-MPT, or most NCR/Symbios SCSI.
  - RAID controllers. Dell PERC (Adaptec RAID or LSI MegaRAID), HP Smart Array RAID, or IBM (Adaptec) ServeRAID controllers.
- SCSI disk or a local, non-network, RAID LUN with unpartitioned space for the virtual machines.
- For Serial ATA (SATA), a disk connected through supported SAS controllers or supported on-board SATA controllers. SATA disks will be considered remote, not local. These disks will not be used as a scratch partition by default because they are seen as remote.

NOTE You cannot connect a SATA CD-ROM device to a virtual machine on an ESXi 5.5 host. To use the SATA CD-ROM device, you must use IDE emulation mode.

Storage Systems

For a list of supported storage systems, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility. ESXi 5.5 supports installing on and booting from the following storage systems:

- SATA disk drives. SATA disk drives connected behind supported SAS controllers or supported on-board SATA controllers.

  Supported SAS controllers include:

  - LSI1068E (LSISAS3442E)
  - LSI1068 (SAS 5)
  - IBM ServeRAID 8K SAS controller
  - Smart Array P400/256 controller
  - Dell PERC 5.0.1 controller

  Supported on-board SATA include:

  - Intel ICH9
  - NVIDIA MCP55
  - ServerWorks HT1000

  NOTE ESXi does not support using local, internal SATA drives on the host server to create VMFS datastores that are shared across multiple ESXi hosts.

- Serial Attached SCSI (SAS) disk drives. Supported for installing ESXi and for storing virtual machines on VMFS partitions.
- Dedicated SAN disk on Fibre Channel or iSCSI

- USB devices. Supported for installing ESXi.
- Software Fibre Channel over Ethernet (FCoE). See "Installing and Booting ESXi with Software FCoE," on page 165.

ESXi Booting Requirements

vSphere 5.5 supports booting ESXi hosts from the Unified Extensible Firmware Interface (UEFI). With UEFI you can boot systems from hard drives, CD-ROM drives, or USB media. Network booting or provisioning with VMware Auto Deploy requires the legacy BIOS firmware and is not available with UEFI.

ESXi can boot from a disk larger than 2TB provided that the system firmware and the firmware on any add-in card that you are using support it. See the vendor documentation.

NOTE Changing the boot type from legacy BIOS to UEFI after you install ESXi 5.5 might cause the host to fail to boot. In this case, the host displays an error message similar to: `Not a VMware boot bank`. Changing the host boot type between legacy BIOS and UEFI is not supported after you install ESXi 5.5.

Storage Requirements for ESXi 5.5 Installation

Installing ESXi 5.5 requires a boot device that is a minimum of 1GB in size. When booting from a local disk or SAN/iSCSI LUN, a 5.2GB disk is required to allow for the creation of the VMFS volume and a 4GB scratch partition on the boot device. If a smaller disk or LUN is used, the installer will attempt to allocate a scratch region on a separate local disk. If a local disk cannot be found the scratch partition, `/scratch`, will be located on the ESXi host ramdisk, linked to `/tmp/scratch`. You can reconfigure `/scratch` to use a separate disk or LUN. For best performance and memory optimization, VMware recommends that you do not leave `/scratch` on the ESXi host ramdisk.

To reconfigure `/scratch`, see the topic "Set the Scratch Partition from the vSphere Web Client" in the *vSphere Installation and Setup* documentation.

Due to the I/O sensitivity of USB and SD devices the installer does not create a scratch partition on these devices. When installing on USB or SD devices, the installer attempts to allocate a scratch region on an available local disk or datastore. If no local disk or datastore is found, `/scratch` is placed on the ramdisk. After the installation, you should reconfigure `/scratch` to use a persistent datastore. Although a 1GB USB/SD device will suffice for a minimal installation, VMware strongly recommends using a 4GB or larger USB/SD device. The extra space will be used for an expanded coredump partition on the USB/SD device. VMware recommends using a high quality USB flash drive of 16GB or larger so that the extra flash cells can prolong the life of the boot media, but high quality drives of 4GB or larger are sufficient to hold the extended coredump partition. See Knowledge Base article 2004784.

In Auto Deploy installations, the installer attempts to allocate a scratch region on an available local disk or datastore. If no local disk or datastore is found `/scratch` is placed on ramdisk. You should reconfigure /scratch to use a persistent datastore following the installation.

For environments that boot from a SAN or use Auto Deploy, it is not necessary to allocate a separate LUN for each ESXi host. You can co-locate the scratch regions for many ESXi hosts onto a single LUN. The number of hosts assigned to any single LUN should be weighed against the LUN size and the I/O behavior of the virtual machines.

Recommendation for Enhanced ESXi Performance

To enhance performance, install ESXi on a robust system with more RAM than the minimum required and with multiple physical disks.

For ESXi system requirements, see "ESXi Hardware Requirements," on page 13. See also the technical papers on vSphere 5 performance at http://www.vmware.com/resources/techresources/cat/91,203,96.

Table 2-1. Recommendations for Enhanced Performance

System Element	Recommendation
RAM	ESXi hosts require more RAM than typical servers. Provide at least 8GB of RAM to take full advantage of ESXi features and run virtual machines in typical production environments. An ESXi host must have sufficient RAM to run concurrent virtual machines. The following examples are provided to help you calculate the RAM required by the virtual machines running on the ESXi host. Operating four virtual machines with Red Hat Enterprise Linux or Windows XP requires at least 3GB of RAM for baseline performance. This figure includes approximately 1024MB for the virtual machines, 256MB minimum for each operating system as recommended by vendors. Running these four virtual machines with 512MB RAM requires that the ESXi host have approximately 4GB RAM, which includes 2048MB for the virtual machines. These calculations do not take into account possible memory savings from using variable overhead memory for each virtual machine. See *vSphere Resource Management* .
Dedicated Fast Ethernet adapters for virtual machines	Place the management network and virtual machine networks on different physical network cards. Dedicated Gigabit Ethernet cards for virtual machines, such as Intel PRO 1000 adapters, improve throughput to virtual machines with high network traffic.
Disk location	Place all data that your virtual machines use on physical disks allocated specifically to virtual machines. Performance is better when you do not place your virtual machines on the disk containing the ESXi boot image. Use physical disks that are large enough to hold disk images that all the virtual machines use.
VMFS5 partitioning	The ESXi installer creates the initial VMFS volumes on the first blank local disk found. To add disks or modify the original configuration, use the vSphere Web Client. This practice ensures that the starting sectors of partitions are 64K-aligned, which improves storage performance. **NOTE** For SAS-only environments, the installer might not format the disks. For some SAS disks, it is not possible to identify whether the disks are local or remote. After the installation, you can use the vSphere Web Client to set up VMFS.
Processors	Faster processors improve ESXi performance. For certain workloads, larger caches improve ESXi performance.
Hardware compatibility	Use devices in your server that are supported by ESXi 5.5 drivers. See the *Hardware Compatibility Guide* at http://www.vmware.com/resources/compatibility.

Hardware Requirements for vCenter Server, the vSphere Web Client , vCenter Inventory Service, and vCenter Single Sign-On

vCenter Server host machines must meet hardware requirements.

vCenter Single Sign-On, the vSphere Web Client , vCenter Inventory Service, and vCenter Server Hardware Requirements

You can install vCenter Single Sign-On, the vSphere Web Client, vCenter Inventory Service, and vCenter Server on the same host machine (as with vCenter Simple Install) or on different machines. See Table 2-2.

The following tables list the hardware requirements for vCenter Single Sign-On and Inventory Service, running on separate host machines.

- Table 2-3
- Table 2-4

If you use Custom Install to install vCenter Single Sign-On, vCenter Inventory Service, and vCenter Server on the same host machine, the vCenter Single Sign-On, and Inventory Service memory and disk storage requirements are in addition to the requirements for vCenter Server. See Table 2-5.

Table 2-2. Minimum Hardware Requirements for Simple Install Deployment of vCenter Single Sign-On, the vSphere Web Client , vCenter Inventory Service, and vCenter Server

Host Hardware for Simple Install Deployment	Minimum Requirement
Processor	Intel or AMD x64 processor with two or more logical cores, each with a speed of 2GHz.
Memory	12GB. Memory requirements are higher if the vCenter Server database runs on the same machine as vCenter Server. vCenter Server includes several Java services: VMware VirtualCenter Management Webservices (tc Server), Inventory Service, and Profile-Driven Storage Service. When you install vCenter Server, you select the size of your vCenter Server inventory to allocate memory for these services. The inventory size determines the maximum JVM heap settings for the services. You can adjust this setting after installation if the number of hosts in your environment changes. See the recommendations in Table 2-7.
Disk storage	100GB recommended. 40-60GB of free disk space are required after installation, depending on the size of your inventory. You should provide more space to allow for future growth of your inventory. Disk storage requirements are higher if the vCenter Server database runs on the same machine as vCenter Server, depending on the size of the database. In vCenter Server 5.x, the default size for vCenter Server logs is 450MB larger than in vCenter Server 4.x. Make sure the disk space allotted to the log folder is sufficient for this increase.
Network speed	1Gbps

Table 2-3. Minimum Hardware Requirements for vCenter Single Sign-On, Running on a Separate Host Machine from vCenter Server

vCenter Single Sign-On Hardware	Requirement
Processor	Intel or AMD x64 processor with two or more logical cores, each with a speed of 2GHz.
Memory	3GB. If vCenter Single Sign-On runs on the same host machine as vCenter Server, see Table 2-2 or Table 2-5.
Disk storage	2GB.
Network speed	1Gbps

Table 2-4. Minimum Hardware Requirements for vCenter Inventory Service, Running on a Separate Host Machine from vCenter Server

vCenter Inventory Service Hardware	Requirement
Processor	Intel or AMD x64 processor with two or more logical cores, each with a speed of 2GHz.
Memory	3GB. If vCenter Inventory Service runs on the same host machine as vCenter Server, see Table 2-2 or Table 2-5.
Disk storage	If vCenter Inventory Service runs on the same host machine as vCenter Server, these requirements are in addition to the disk space required for vCenter Server and any other applications running on the vCenter Server host machine. See Table 2-5. Disk storage requirements for Inventory Service depend on inventory size and the amount of activity in the virtual machines in the inventory. At typical activity rates, Inventory Service uses 6GB - 12GB of disk space for 15,000 virtual machines distributed among 1,000 hosts. A high rate of activity (more than 20 percent of your virtual machines changing per hour) results in write-ahead logs (WAL) being written to disk to handle updates, instead of in-line writes into existing disk usage. This high rate of activity is often associated with Virtual Desktop Infrastructure (VDI) use cases. In the following guidelines for required disk space, a small inventory is 1-100 hosts or 1-1000 virtual machines, and a large inventory is more than 400 hosts or 4000 virtual machines. ■ Small inventory, low activity rate: 5GB. ■ Small inventory, high activity rate: 15GB. ■ Large inventory, low activity rate: 15GB. ■ Large inventory, high activity rate: 40GB-60GB.
Network speed	1Gbps

Table 2-5. Minimum Hardware Requirements for vCenter Server

vCenter Server Hardware	Requirement
CPU	Two 64-bit CPUs or one 64-bit dual-core processor.
Processor	2.0GHz or faster Intel 64 or AMD 64 processor. The Itanium (IA64) processor is not supported. Processor requirements might be higher if the database runs on the same machine.

Table 2-5. Minimum Hardware Requirements for vCenter Server (Continued)

vCenter Server Hardware	Requirement
Memory	The amount of memory needed depends on your vCenter Server configuration. ■ If vCenter Server is installed on a different host machine than vCenter Single Sign-On and vCenter Inventory Service, 4GB of RAM are required. ■ If vCenter Server, vCenter Single Sign-On and vCenter Inventory Service are installed on the same host machine (as with vCenter Simple Install), 10GB of RAM are required. Memory requirements are higher if the vCenter Server database runs on the same machine as vCenter Server. vCenter Server includes several Java services: VMware VirtualCenter Management Webservices (tc Server), Inventory Service, and Profile-Driven Storage Service. When you install vCenter Server, you select the size of your vCenter Server inventory to allocate memory for these services. The inventory size determines the maximum JVM heap settings for the services. You can adjust this setting after installation if the number of hosts in your environment changes. See the recommendations in Table 2-7.
Disk storage	The amount of disk storage needed for the vCenter Server installation depends on your vCenter Server configuration. ■ If vCenter Server is installed on a different host machine than vCenter Single Sign-On and vCenter Inventory Service, 4GB are required. ■ If vCenter Server, vCenter Single Sign-On and vCenter Inventory Service are installed on the same host machine (as with vCenter Simple Install), at least 40-60GB of free disk space are required after installation, depending on the size of your inventory. You should provide more space to allow for future growth of your inventory. For guidelines about the disk space required for vCenter Single Sign-On and Inventory Service, see Table 2-3 and Table 2-4 Disk storage requirements are higher if the vCenter Server database runs on the same machine as vCenter Server, depending on the size of those databases. In vCenter Server 5.x, the default size for vCenter Server logs is 450MB larger than in vCenter Server 4.x. Make sure the disk space allotted to the log folder is sufficient for this increase.
Microsoft SQL Server 2008 R2 Express disk	Up to 2GB free disk space to decompress the installation archive. Approximately 1.5GB of these files are deleted after the installation is complete.
Network speed	1Gbps

NOTE Installing vCenter Server on a network drive or USB flash drive is not supported.

For the hardware requirements of your database, see your database documentation. The database requirements are in addition to the vCenter Server requirements if the database and vCenter Server run on the same machine.

vSphere Web Client Hardware Requirements

The vSphere Web Client has two components: A Java server and an Adobe Flex client application running in a browser.

Table 2-6. Hardware Requirements for the vSphere Web Client Server Component

vSphere Web Client Server Hardware	Requirement
Memory	At least 2GB: 1GB for the Java heap, and 1GB for ■ The resident code ■ The stack for Java threads ■ Global/bss segments for the Java process
CPU	2GHz processor with two or more cores
Disk Storage	At least 2GB free disk space
Networking	Gigabit connection recommended

JVM heap settings for vCenter Server

The JVM heap settings for vCenter Server depend on your inventory size. See "Configuring VMware vCenter Server - tc Server Settings in vCenter Server," on page 137.

Table 2-7. JVM Heap Settings for vCenter Server

vCenter Server Inventory	VMware VirtualCenter Management Webservices (tc Server)	Inventory Service	Profile-Driven Storage Service
Small inventory (1-100 hosts or 1-1000 virtual machines)	1GB	3GB	1GB
Medium inventory (100-400 hosts or 1000-4000 virtual machines)	2GB	6GB	2GB
Large inventory (More than 400 hosts or 4000 virtual machines)	3GB	12GB	4GB

VMware vCenter Server Appliance Hardware Requirements and Recommendations

Table 2-8. Hardware Requirements for VMware vCenter Server Appliance

VMware vCenter Server Appliance Hardware	Requirement
Disk storage on the host machine	For most deployments, the vCenter Server Appliance requires at least 70GB of disk space, and is limited to a maximum size of 125GB. The required disk space depends on the size of your vCenter Server inventory. The vCenter Server Appliance can be deployed with thin-provisioned virtual disks that can grow to the maximum size of 125GB. If the host machine does not have enough free disk space to accommodate the growth of the vCenter Server Appliance virtual disks, vCenter Server might cease operation, and you will not be able to manage your vSphere environment.
Memory in the VMware vCenter Server Appliance	Using the embedded PostgreSQL database, the vCenter Server Appliance supports up to 100 hosts or 3000 virtual machines, and has the following memory requirements ■ Very small inventory (10 or fewer hosts, 100 or fewer virtual machines): at least 8GB. ■ Small inventory (10-50 hosts or 100-1500 virtual machines): at least 16GB. ■ Medium inventory (the maximum inventory supported with the embedded database; 50-100 hosts or 1500-3000 virtual machines): at least 24GB. Using an external Oracle database, the vCenter Server Appliance supports up to 1000 hosts or 10000 registered virtual machines, and 10000 powered-on virtual machines, and has the following memory requirements: ■ Very small inventory (10 or fewer hosts, 100 or fewer virtual machines): at least 4GB. ■ Small inventory (10-100 hosts or 100-1000 virtual machines): at least 8GB. ■ Medium inventory (100-400 hosts or 1000-4000 virtual machines): at least 16GB. ■ Large inventory (More than 400 hosts or 4000 virtual machines): at least 32GB.

For inventory and other configuration limits in the vCenter Server Appliance, see *Configuration Maximums*.

Table 2-9. JVM Heap Settings for VMware vCenter Server Appliance

vCenter Server Appliance Inventory	VMware VirtualCenter Management Webservices (tc Server)	Inventory Service	Profile-Driven Storage Service
Small inventory (1-100 hosts or 1-1000 virtual machines)	512MB	3GB	1GB
Medium inventory (100-400 hosts or 1000-4000 virtual machines)	512MB	6GB	2GB
Large inventory (More than 400 hosts or 4000 virtual machines)	1GB	12GB	4GB

See "Configuring VMware vCenter Server - tc Server Settings in vCenter Server," on page 137.

vCenter Server Software Requirements

Make sure that your operating system supports vCenter Server. vCenter Server requires a 64-bit operating system, and the 64-bit system DSN is required for vCenter Server to connect to its database.

For a list of supported operating systems, see the VMware Compatibility Guide at http://www.vmware.com/resources/compatibility. In the drop-down **What are you looking for** menu on that page, select **Host OS** and use the selection boxes to find compatible operating systems for your version of vCenter Server.

vCenter Server requires the Microsoft .NET 3.5 SP1 Framework. If it is not installed on your system, the vCenter Server installer installs it. The .NET 3.5 SP1 installation might require Internet connectivity to download more files.

NOTE If your vCenter Server host machine uses a non-English operating system, install both the Microsoft .NET Framework 3.5 SP1 and Microsoft .NET Framework 3.5 Language Pack through Windows Update. Windows Update automatically selects the correct localized version for your operating system. The .NET Framework installed through the vCenter Server installer includes only the English version.

vCenter Server 5.5 removes support for Windows Server 2003 as a host operating system. See the VMware Compatibility Guide at http://www.vmware.com/resources/compatibility/search.php.

vCenter Server 5.5 removes support for Windows Server 2008 SP1 as a host operating system. Upgrade Windows Server 2008 SP1 hosts to SP2 before upgrading vCenter Server to version 5.5. See the VMware Compatibility Guide at http://www.vmware.com/resources/compatibility/search.php and the Microsoft Software Lifecycle Policy at http://support.microsoft.com/lifecycle/#ServicePackSupport.

If you plan to use the Microsoft SQL Server 2008 R2 Express database that is bundled with vCenter Server, Microsoft Windows Installer version 4.5 (MSI 4.5) is required on your system. You can download MSI 4.5 from the Microsoft Web site. You can also install MSI 4.5 directly from the vCenter Server `autorun.exe` installer.

The VMware vCenter Server Appliance can be deployed only on hosts that are running ESX version 4.x or ESXi version 4.x or later.

vSphere Web Client Software Requirements

Make sure that your browser supports the vSphere Web Client.

VMware has tested and supports the following guest operating systems and browser versions for the vSphere Web Client.

Table 2-10. Supported guest operating systems and browser versions for the vSphere Web Client .

Operating system	Browser
Windows 32-bit and 64-bit	Microsoft Internet Explorer 8, 9 (64-bit only), and 10. Mozilla Firefox: the latest browser version, and the one previous version at the time the vSphere 5.5 is produced. Google Chrome: the latest browser version, and the one previous version at the time the vSphere 5.5 is produced.
Mac OS	Mozilla Firefox: the latest browser version, and the one previous version at the time the vSphere 5.5 is produced. Google Chrome: the latest browser version, and the one previous version at the time the vSphere 5.5 is produced.

Later versions of these browsers are likely to work, but have not been tested.

The vSphere Web Client requires the Adobe Flash Player version 11.5.0 or later to be installed with the appropriate plug-in for your browser.

Providing Sufficient Space for System Logging

ESXi 5.x uses a new log infrastructure. If your host is deployed with Auto Deploy, or if you set up a log directory separate from the default location in a scratch directory on the VMFS volume, you might need to change your current log size and rotation settings to ensure that enough space for system logging exists.

All vSphere components use this infrastructure. The default values for log capacity in this infrastructure vary, depending on the amount of storage available and on how you have configured system logging. Hosts that are deployed with Auto Deploy store logs on a RAM disk, which means that the amount of space available for logs is small.

If your host is deployed with Auto Deploy, reconfigure your log storage in one of the following ways:

- Redirect logs over the network to a remote collector.
- Redirect logs to a NAS or NFS store.

You might also want to reconfigure log sizing and rotations for hosts that are installed to disk, if you redirect logs to nondefault storage, such as a NAS or NFS store.

You do not need to reconfigure log storage for ESXi hosts that use the default configuration, which stores logs in a scratch directory on the VMFS volume. For these hosts, ESXi 5.x autoconfigures logs to best suit your installation, and provides enough space to accommodate log messages.

Table 2-11. Recommended Minimum Size and Rotation Configuration for hostd, vpxa, and fdm Logs.

Log	Maximum Log File Size	Number of Rotations to Preserve	Minimum Disk Space Required
Management Agent (hostd)	10240KB	10	100MB
VirtualCenter Agent (vpxa)	5120KB	10	50MB
vSphere HA agent (Fault Domain Manager, fdm)	5120KB	10	50MB

For information about setting up and configuring syslog and a syslog server and installing vSphere Syslog Collector, see the *vSphere Installation and Setup* documentation.

Required Ports for vCenter Server

The VMware vCenter Server system must be able to send data to every managed host and receive data from every vSphere Web Client. To enable migration and provisioning activities between managed hosts, the source and destination hosts must be able to receive data from each other.

For information about ports required for the vCenter Server Appliance, see "Required Ports for the vCenter Server Appliance," on page 26.

VMware uses designated ports for communication. Additionally, the managed hosts monitor designated ports for data from the vCenter Server system. If a firewall exists between any of these elements and Windows firewall service is in use, the installer opens the ports during the installation. For custom firewalls, you must manually open the required ports. If you have a firewall between two managed hosts and you want to perform source or target activities, such as migration or cloning, you must configure a means for the managed hosts to receive data.

NOTE In Microsoft Windows Server 2008, a firewall is enabled by default.

Table 2-12. Ports Required for Communication Between Components

Port	Description
22	SSH Server (vSphere Client)
53	DNS Client
80	vCenter Server requires port 80 for direct HTTP connections. Port 80 redirects requests to HTTPS port 443. This redirection is useful if you accidentally use http://server instead of https://server. WS-Management (also requires port 443 to be open) If you use a custom Microsoft SQL database (not the bundled SQL Server 2008 database) that is stored on the same host machine as the vCenter Server, port 80 is used by the SQL Reporting Service. When you install vCenter Server, the installer will prompt you to change the HTTP port for vCenter Server. Change the vCenter Server HTTP port to a custom value to ensure a successful installation. Microsoft Internet Information Services (IIS) also use port 80. See "Conflict Between vCenter Server and IIS for Port 80," on page 27.
88	Control interface RPC for Kerberos, used by vCenter Single Sign-On
111	RPC service that is used for the NIS register by the vCenter Server Appliance
123	NTP Client
135	Used to join vCenter Virtual Appliance to an Active Directory domain.
161	SNMP Server
389	This port must be open on the local and all remote instances of vCenter Server. This is the LDAP port number for the Directory Services for the vCenter Server group. The vCenter Server system needs to bind to port 389, even if you are not joining this vCenter Server instance to a Linked Mode group. If another service is running on this port, it might be preferable to remove it or change its port to a different port. You can run the LDAP service on any port from 1025 through 65535. If this instance is serving as the Microsoft Windows Active Directory, change the port number from 389 to an available port from 1025 through 65535.
427	The CIM client uses the Service Location Protocol, version 2 (SLPv2) to find CIM servers.
443	The default port that the vCenter Server system uses to listen for connections from the vSphere Client. To enable the vCenter Server system to receive data from the vSphere Client, open port 443 in the firewall. The vCenter Server system also uses port 443 to monitor data transfer from SDK clients. This port is also used for the following services: ■ WS-Management (also requires port 80 to be open) ■ vSphere Client access to vSphere Update Manager ■ Third-party network management client connections to vCenter Server ■ Third-party network management clients access to hosts
513	vCenter Virtual Appliance used for logging activity
636	For vCenter Server Linked Mode, this is the SSL port of the local instance. If another service is running on this port, it might be preferable to remove it or change its port to a different port. You can run the SSL service on any port from 1025 through 65535.
902	The default port that the vCenter Server system uses to send data to managed hosts. Managed hosts also send a regular heartbeat over UDP port 902 to the vCenter Server system. This port must not be blocked by firewalls between the server and the hosts or between hosts. Port 902 must not be blocked between the vSphere Client and the hosts. The vSphere Client uses this port to display virtual machine consoles
903	Access a virtual machine console from the vSphere Client when the vSphere Client is connected directly to the ESXi host (no vCenter Server). MKS transactions (xinetd/vmware-authd-mks)
1234, 1235	vSphere Replication
2012	Control interface RPC for vCenter Single Sign-On vmdir.
2013	Control interface RPC for Kerberos, used by vCenter Single Sign-On
2014	RPC port for all VMCA (VMware Certificate Authority) APIs

Table 2-12. Ports Required for Communication Between Components (Continued)

Port	Description
2049	Transactions from NFS storage devices This port is used on the VMkernel interface.
3260	Transactions to iSCSI storage devices
3268	Default port for Active Directory multi-domain controller deployments
3269	Default SSL port for Active Directory multi-domain controller deployments
5900-5964	RFB protocol, which is used by management tools such as VNC
5988	CIM transactions over HTTP
5989	CIM XML transactions over HTTPS
6501	Auto Deploy service
6502	Auto Deploy management
7005	vCenter Single Sign-On
7009	vCenter Single Sign-On
7080	vCenter Single Sign-On
7331	vSphere Web Client - HTML5 Remote Console
7444	vCenter Single Sign-On HTTPS
8000	Requests from vMotion
8009	AJP connector port for vCenter Server Appliance communication with Tomcat
8080	Web Services HTTP. Used for the VMware VirtualCenter Management Web Services.
8100	Traffic between hosts for vSphere Fault Tolerance (FT)
8182	Traffic between hosts for vSphere High Availability (HA)
8200	Traffic between hosts for vSphere Fault Tolerance (FT)
8443	Web Services HTTPS. Used for the VMware VirtualCenter Management Web Services.
9009	Used to allow a vCenter Server Appliance to communicate with the vSphere Web Client.
9090	vSphere Web Client HTTP
9443	vSphere Web Client HTTPS
9875 - 9877	vSphere Web Client Java Management Extension (JMX). Dynamically acquired upon the vSphere Web Client service starting.
10080	vCenter Inventory Service HTTP
10109	vCenter Inventory Service Management
10111	vCenter Inventory Service Linked Mode Communication
10443	vCenter Inventory Service HTTPS
11711	vCenter Single Sign-On LDAP
11712	vCenter Single Sign-On LDAPS
12721	VMware Identity Management service
49000 - 65000	vCenter Single Sign-On - VMware Identity Management Service. Dynamically acquired when the VMware Identity Management Service starts.
60099	Web Service change service notification port

To have the vCenter Server system use a different port to receive vSphere Web Client data, see the *vCenter Server and Host Management* documentation.

For a discussion of firewall configuration, see the *vSphere Security* documentation.

Required Ports for the vCenter Server Appliance

The VMware vCenter Server system must be able to send data to every managed host and receive data from every vSphere Web Client. For migration and provisioning activities between managed hosts, the source and destination hosts must be able to receive data from each other.

For information about ports required for vCenter Server on Windows, see "Required Ports for vCenter Server," on page 23.

VMware uses designated ports for communication. Additionally, the managed hosts monitor designated ports for data from the vCenter Server system. The vCenter Server Appliance is preconfigured to use the ports listed in Table 2-13. For custom firewalls, you must manually open the required ports. If you have a firewall between two managed hosts and you want to perform source or target activities, such as migration or cloning, you must configure a means for the managed hosts to receive data.

Table 2-13. Ports Required for the vCenter Server Appliance

Port	Description
80	vCenter Server requires port 80 for direct HTTP connections. Port 80 redirects requests to HTTPS port 443. This redirection is useful if you accidentally use http://server instead of https://server.
443	The vCenter Server system uses port 443 to monitor data transfer from SDK clients.
902	The default port that the vCenter Server system uses to send data to managed hosts. Managed hosts also send a regular heartbeat over UDP port 902 to the vCenter Server system. This port must not be blocked by firewalls between the server and the hosts or between hosts.
8080	Web Services HTTP. Used for the VMware VirtualCenter Management Web Services.
8443	Web Services HTTPS. Used for the VMware VirtualCenter Management Web Services.
10080	vCenter Inventory Service HTTP
10443	vCenter Inventory Service HTTPS
10109	vCenter Inventory Service database
514	vSphere Syslog Collector server
1514	vSphere Syslog Collector server (SSL)
6500	Network coredump server (UDP)
6501	Auto Deploy service
6502	Auto Deploy management
9090	vSphere Web Client HTTP
9443	vSphere Web Client HTTPS
5480	vCenter Server Appliance Web user interface HTTPS
5489	vCenter Server Appliance Web user interface CIM service
22	System port for SSHD

To have the vCenter Server system use a different port to receive vSphere Web Client data, see the *vCenter Server and Host Management* documentation.

For a discussion of firewall configuration, see the *vSphere Security* documentation.

Conflict Between vCenter Server and IIS for Port 80

vCenter Server and Microsoft Internet Information Service (IIS) both use port 80 as the default port for direct HTTP connections. This conflict can cause vCenter Server to fail to restart after the installation of vSphere Authentication Proxy.

Problem

vCenter Server fails to restart after the installation of vSphere Authentication Proxy is complete.

Cause

If you do not have IIS installed when you install vSphere Authentication Proxy, the installer prompts you to install IIS. Because IIS uses port 80, which is the default port for vCenter Server direct HTTP connections, vCenter Server fails to restart after the installation of vSphere Authentication Proxy is complete. See "Required Ports for vCenter Server," on page 23.

Solution

- To resolve a conflict between IIS and vCenter Server for port 80, take one of the following actions.

Option	Description
If you installed IIS before installing vCenter Server	Change the port for vCenter Server direct HTTP connections from 80 to another value.
If you installed vCenter Server before installing IIS	Before restarting vCenter Server, change the binding port of the IIS default Web site from 80 to another value.

DNS Requirements for vSphere

You install vCenter Server, like any other network server, on a machine with a fixed IP address and well-known DNS name, so that clients can reliably access the service.

Assign a static IP address and host name to the Windows server that will host the vCenter Server system. This IP address must have a valid (internal) domain name system (DNS) registration.

Ensure that the ESXi host management interface has a valid DNS resolution from the vCenter Server and all vSphere Web Clients. Ensure that the vCenter Server has a valid DNS resolution from all ESXi hosts and all vSphere Web Clients.

Ensure that the vCenter Server is installed on a machine that has a resolvable fully qualified domain name (FQDN). To check that the FQDN is resolvable, type **`nslookup`** ***`your_vCenter_Server_fqdn`*** at a command line prompt. If the FQDN is resolvable, the **`nslookup`** command returns the IP and name of the domain controller machine.

Ensure that DNS reverse lookup returns a fully qualified domain name when queried with the IP address of the vCenter Server. When you install vCenter Server, the installation of the web server component that supports the vSphere Web Client fails if the installer cannot look up the fully qualified domain name of the vCenter Server from its IP address. Reverse lookup is implemented using PTR records. To create a PTR record, see the documentation for your vCenter Server host operating system.

If you use DHCP instead of a static IP address for vCenter Server, make sure that the vCenter Server computer name is updated in the domain name service (DNS). Ping the computer name to test the connection. For example, if the computer name is `host-1.company.com`, run the following command in the Windows command prompt:

```
ping host-1.company.com
```

If you can ping the computer name, the name is updated in DNS.

Supported Remote Management Server Models and Minimum Firmware Versions

You can use remote management applications to install ESXi or for remote management of hosts.

Table 2-14. Supported Remote Management Server Models and Firmware Versions

Remote Controller Make and Model	Firmware Version	Java
Dell DRAC 6	1.54 (Build 15), 1.70 (Build 21)	1.6.0_24
Dell DRAC 5	1.0, 1.45, 1.51	1.6.0_20,1.6.0_203
Dell DRAC 4	1.75	1.6.0_23
HP ILO	1.81, 1.92	1.6.0_22, 1.6.0_23
HP ILO 2	1.8, 1.81	1.6.0_20, 1.6.0_23
IBM RSA 2	1.03, 1.2	1.6.0_22

Update Manager Hardware Requirements

You can run Update Manager on any system that meets the minimum hardware requirements.

Minimum hardware requirements for Update Manager vary depending on how Update Manager is deployed. If the database is installed on the same machine as Update Manager, requirements for memory size and processor speed are higher. To ensure acceptable performance, verify that your system meets the minimum hardware requirements.

Table 2-15. Minimum Hardware Requirements

Hardware	Requirements
Processor	Intel or AMD x86 processor with two or more logical cores, each with a speed of 2GHz
Network	10/100 Mbps
	For best performance, use a Gigabit connection between Update Manager and the ESX/ESXi hosts
Memory	2GB RAM if Update Manager and vCenter Server are on different machines
	4GB RAM if Update Manager and vCenter Server are on the same machine

Update Manager uses a SQL Server or Oracle database. You should use a dedicated database for Update Manager, not a database shared with vCenter Server, and should back up the database periodically. Best practice is to have the database on the same computer as Update Manager or on a computer in the local network.

Depending on the size of your deployment, Update Manager requires a minimum amount of free space per month for database usage. For more information about space requirements, see the *VMware vSphere Update Manager Sizing Estimator*.

For more information about ESXi 5.x and vCenter Server 5.x hardware requirements, see Chapter 2, "System Requirements," on page 13.

Supported Operating Systems and Database Formats

Update Manager works with specific databases and operating systems.

The Update Manager server requires a 64-bit Windows system.

NOTE Make sure the system on which you are installing the Update Manager server is not an Active Directory domain controller.

The Update Manager plug-in requires the vSphere Client, and works with the same operating systems as the vSphere Client.

Update Manager scans and remediates Windows and Linux virtual machines for VMware Tools and virtual hardware upgrades.

The Update Manager server requires SQL Server or Oracle database. Update Manager can handle small-scale environments using the bundled SQL Server 2008 R2 Express. For environments with more than 5 hosts and 50 virtual machines, create either an Oracle or a SQL Server database for Update Manager. For large scale environments, you should set up the Update Manager database on a different computer than the Update Manager server and the vCenter Server database.

To see a list of operating systems on which you can install the Update Manager server and the UMDS, select the **Host OS** option from the *vSphere Compatibility Guide* at http://www.vmware.com/resources/compatibility/search.php.

To see a list of database formats that are compatible with the Update Manager server and the UMDS, select the **Solution/Database Interoperability** option from the *VMware Product Interoperability Matrixes* at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Preparing for the Upgrade to vCenter Server 3

Before you upgrade to vCenter Server, make sure your system is properly prepared.

To ensure that your system is prepared for the upgrade, read all the subtopics in this section.

This chapter includes the following topics:

- "Microsoft SQL Database Set to Unsupported Compatibility Mode Causes vCenter Server Installation or Upgrade to Fail," on page 59

About the vCenter Server Upgrade

VMware supports in-place upgrades on 64-bit systems from vCenter Server 4.x, vCenter Server 5.0.x, and vCenter Server 5.1.x to vCenter Server 5.5.

Unlike versions before vCenter Server 5.1, vCenter Server 5.5 does not support directly migrating an existing, 5.0.x or earlier vCenter Server to a new machine during an upgrade to version 5.5. You can migrate such an existing vCenter Server to a new machine during an upgrade to version 5.0.x, and then perform an in-place upgrade from version 5.0.x to version 5.5. See "Upgrading to vCenter Server on a Different Machine," on page 52.

vCenter Server 5.5 can manage ESX 4.x/ESXi 4.x, ESXi 5.0.x, and 5.1 x hosts in the same cluster with ESXi 5.5 hosts. vCenter Server 5.5 cannot manage ESX 2.x or 3.x hosts.

NOTE You cannot upgrade a vCenter Server 4.x instance that is running on Windows XP Professional x64 Edition to vCenter Server 5.5, because vCenter Server 5.5 does not support Windows XP Professional x64.

vSphere 5.1 introduced vCenter Single Sign On service as part of the vCenter Server management infrastructure. This change affects vCenter Server installation, upgrading, and operation. See "How vCenter Single Sign-On Affects vCenter Server Upgrades," on page 32

How vCenter Single Sign-On Affects vCenter Server Upgrades

Which users can log in to vCenter Server after an upgrade depends on the version that you are upgrading from and the deployment configuration.

In upgrades to vCenter Server 5.0 and earlier, which do not include a vCenter Single Sign-On service, both the local operating system users and Active Directory users that are registered with vCenter Server continue to work with the upgraded vCenter Server.

This behavior changes if you are upgrading from a version that does not include vCenter Single Sign-On to a version that does include vCenter Single Sign-On: vCenter Server version 5.1 or vCenter Server version 5.5.

NOTE With vCenter Single Sign-On, local operating system users become far less important than the users in a directory service such as Active Directory. As a result, it is not always possible, or even desirable, to keep local operating system users as authenticated users.

After the upgrade from a version earlier than version 5.1, you might be prompted for the administrator of the root folder in the vSphere inventory hierarchy during installation. This might happen because of changes in user stores from pre-5.1 versions to 5.1 and later versions of vSphere. See "Hierarchical Inheritance of Permissions," on page 107.

Simple Install Upgrade

A Simple Install upgrade installs or upgrades a single vCenter Server and related components.

If you upgrade to vCenter Server 5.5 from a vCenter Server version that does not include vCenter Single Sign-On, vCenter Single Sign-On recognizes existing local operating system users. In addition, the user administrator@vsphere.local can log in as an administrator user to vCenter Single Sign-On and vCenter Server. If your previous installation supported Active Directory users, you can add the Active Directory domain as an identity source.

If you upgrade vCenter Single Sign-On and vCenter Server, vCenter Single Sign-On recognizes existing local operating system users. In addition, the user administrator@vsphere.local can log in to vCenter Single Sign-On and vCenter Server as an administrator user. If your previous installation included an Active Directory domain as an identity source, that identity source is still available after the upgrade. Because vCenter Server supports only one default identity source, users might have to specify the domain when they log in (*DOMAIN\user*).

Custom Upgrade

A custom upgrade might install different vCenter Server components on different machines or install a second vCenter Server system on the same machine. You also use Custom Install to upgrade an environment that is installed in different locations.

If you upgrade to vCenter Server 5.5 from a vCenter Server version that does not include vCenter Single Sign-On, and you install vCenter Single Sign-On on a different machine than vCenter Server, vCenter Single Sign-On does not recognize existing local operating system users. The user administrator@vsphere.local can log in to vCenter Single Sign-On and vCenter Server as an administrator user. If your previous installation supported Active Directory users, you can add the Active Directory domain as an identity source.

If you are upgrading vCenter Server from a version that includes vCenter Single Sign-On in multisite mode, and if the different vCenter Server systems use Linked mode, you must resynchronize first. You can then upgrade all vCenter Single Sign-On instances and maintain Linked Mode functionality. Linked Mode is required for a single view of all vCenter Server systems. Multisite vCenter Single Sign-On is supported only if all nodes are the same version.

If you are upgrading vCenter Server from a version that includes vCenter Single Sign-On in high availability mode, you must upgrade all of the vCenter Single Sign-On high availability instances. Perform the upgrade first, and configure high availability by protecting both vCenter Server and vCenter Single Sign-On with VMware HA or VMware Heartbeat after the upgrade is complete.

NOTE When you install the vCenter Single Sign-On component that is included with vCenter Server version 5.5 in multiple locations, the VMware Directory Service is updated for all vCenter Single Sign-On instances if you make a change in one location.

vCenter Single Sign-On Deployment Modes

vCenter Server provides several ways to deploy vCenter Single Sign-On to best serve your vSphere environment

You can deploy vCenter Single Sign-On in one of three modes.

To choose the right mode for your environment, consider the way you use vCenter Server.

Table 3-1. Choosing a vCenter Single Sign-On Deployment Mode

vCenter Server Deployment	Single Sign-On Deployment Mode
Single vCenter Server	Basic vCenter Single Sign-On
Multiple local vCenter Servers	Basic vCenter Single Sign-On
Multiple remote vCenter Servers	Basic vCenter Single Sign-On

Table 3-1. Choosing a vCenter Single Sign-On Deployment Mode (Continued)

vCenter Server Deployment	Single Sign-On Deployment Mode
Multiple vCenter Servers in Linked Mode	Multisite vCenter Single Sign-On
vCenter Servers with high availability	Basic vCenter Single Sign-On with VMware vSphere HA (provides high availability for vCenter Server and vCenter Single Sign-On) Basic vCenter Single Sign-On with vCenter Server Heartbeat (provides high availability for vCenter Server and vCenter Single Sign-On) See "vCenter Single Sign-On and High Availability," on page 35.

Basic

Basic vCenter Single Sign-On is the most common deployment mode, and meets the requirements of most vSphere 5.1 and 5.5 users. Typically, this deployment mode maintains the same architecture as previous vCenter Server environments. In most cases, you can use vCenter Simple Install to deploy vCenter Server with vCenter Single Sign-On in basic mode.

In Basic deployment mode, a single standalone instance of the vCenter Single Sign-On server supports the connectivity of Active Directory, OpenLDAP, Local Operating System, and vCenter Single Sign-On embedded users and groups. In most cases, the vCenter Single Sign-On instance is installed on the same host machine as vCenter Server, as with the vCenter Server Simple Install option, or the vCenter Server Appliance.

The Basic vCenter Single Sign-On deployment is appropriate in the following circumstances:

- If you have a single vCenter Server of any supported inventory size: up to 1,000 hosts or 10,000 virtual machines.
- If you have multiple geographically dispersed locations, each with a local vCenter Server and you do not require a single-pane-of-glass view as provided by vCenter Linked Mode.

Multiple Single Sign-On instances in the same location

For this deployment mode, you install a vCenter Single Sign-On primary instance and one or more additional vCenter Single Sign-On nodes. Both the primary and high availability instances are placed behind a third-party network load balancer (for example, Apache HTTPD or vCNS). Each vCenter Single Sign-On has its own VMware Directory Service that replicates information with other vCenter Single Sign-On servers. vCenter Single Sign-On administrator users, when connected to vCenter Server through the vSphere Web Client, will see the primary vCenter Single Sign-On instance.

This deployment mode has the following limitations:

- It provides failover only for the vCenter Single Sign-On service. It does not provide failover for the vCenter Single Sign-On host machine.
- It supports the connectivity of Active Directory, OpenLDAP and vCenter Single Sign-On embedded users and groups, but does not support the use of local operating system user accounts.

See "vCenter Single Sign-On and High Availability," on page 35 for high availability options.

Multiple Single Sign-On instances in different locations

This mode is designed for vCenter Server deployments with multiple physical locations. Multisite deployment is required when a single administrator needs to administer vCenter Server instances that are deployed on geographically dispersed sites in Linked Mode.

Each site is represented by one vCenter Single Sign-On instance, with one vCenter Single Sign-On server, or a high-availability cluster. The vCenter Single Sign-On site entry point is the machine that other sites communicate with. This is the only machine that needs to be visible from the other sites. In a clustered deployment, the entry point of the site is the machine where the load balancer is installed.

NOTE This deployment mode is required if you have geographically dispersed vCenter Servers in Linked Mode. You might also consider this mode in the following cases:

- If multiple vCenter Servers require the ability to communicate with each other.
- If you require one vCenter Single Sign-On server security domain for your organization.

This deployment mode has the following limitations:

- It supports the connectivity of Active Directory, OpenLDAP and vCenter Single Sign-On embedded users and groups, but does not support the use of local operating system user accounts.
- Secondary vCenter Single Sign-On instances must belong to the same Active Directory or OpenLDAP domain as the primary vCenter Single Sign-On server and must have a local domain controller available.

You can install the vCenter Single Sign-On nodes in this deployment in any order. Any node that is installed after the first node can point to any node that is already installed. For example, the third node can point to either the first or second node.

vCenter Single Sign-On and High Availability

vSphere provides several ways to ensure availability of your vSphere deployment with vCenter Single Sign-On.

vCenter Single Sign-On is merely an authentication component for vCenter Server. Single Sign-On protection does not provide any benefit without vCenter Server protection. Protecting one without the other does not provide an effective availability solution. The solution you choose to protect vCenter Server will provide the same protection for vCenter Single Sign-On without the additional complexity caused by including third-party technologies.

Options for Protecting vCenter Single Sign-On and vCenter Server

The following options vary in the level of protection afforded, and in the recovery time required.

Backup and restore

Backup and restore should be an essential part of any availability solution, providing a granular recovery method, by tape, disk, or snapshot. However, the recovery time is typically measured in hours or days and requires manual intervention. Any backup solution must be independent of vCenter Server. Solutions like VMware Data Protection require an operational vCenter Server with a functioning vCenter Single Sign-On server to restore a virtual machine.

vSphere HA

vSphere HA is an industry standard for maintaining uptime of virtual machines and for detection of ESXi host failure. Also, with vSphere HA, a failed response to a configured VMware Tools heartbeat automatically reboots the virtual machine onto another operational host within the vSphere cluster. This detection usually occurs within seconds. A virtual machine can be fully rebooted within minutes, providing redundancy for vSphere host failures and virtual machine operating system crashes. vSphere HA does not have any knowledge of the application running inside the virtual machine.

vCenter Server Heartbeat

This separately licensed vCenter Server plug-in provides vCenter Server protection (physical or virtual) and can protect against failure of hosts. vCenter Server Heartbeat also adds application-level monitoring and intelligence of all vCenter Server components. vCenter Server Heartbeat is installed directly onto the vCenter Server or vCenter Server component, and replicates changes to a cloned virtual machine. The cloned virtual machine can take over when a failure event is triggered. The recovery can be accomplished by restarting the component, by restarting the entire application, or by the entire failover of the component or application to one or more paired virtual machines. Recovery time is measured in minutes.

vCenter Single Sign-On Deployment Modes and High Availability

To determine the best deployment mode for vCenter Single Sign-On availability, consider the environment that vCenter Single Sign-On will serve.

Single vCenter Server with local vCenter Single Sign-On in Basic deployment mode

In the simplest deployment of vCenter Single Sign-On for high availability, you install vCenter Single Sign-On in Basic deployment mode, local to vCenter Server, and then add the availability solution. If the single machine that hosts vCenter Server and vCenter Single Sign-On is virtual, you can place it in a vSphere HA-enabled cluster and protect it with no further configuration. If you require protection at the application level, you can use vCenter Server Heartbeat. If vCenter Server and vCenter Single Sign-On are hosted on a physical server, vCenter Server Heartbeat is the only solution for availability.

Multiple vCenter Servers in a single location

In this environment, a dedicated, standalone vCenter Single Sign-On instance serves multiple vCenter Server instances in one physical location. If vCenter Single Sign-On is hosted on a virtual machine, you can place the standalone vCenter Single Sign-On server in a vSphere HA-enabled cluster and protect vCenter Single Sign-On with no further configuration. If you require application-level protection, you can use vCenter Server Heartbeat.

vCenter Server Heartbeat is the only solution for availability if vCenter Single Sign-On is on a physical server. With either vSphere HA or vCenter Server Heartbeat, this deployment provides complete protection of the centralized vCenter Single Sign-On environment.

Geographically dispersed vCenter Servers

If your vSphere deployment includes vCenter Servers in different locations, it is not advisable to use a remote centralized vCenter Single Sign-On environment for vCenter Server authentication. Instead, you can provide one or more vCenter Single Sign-On instances at each location. Depending on the deployment of vCenter Servers at each location, you can use one of the same availability strategies described above in the options "Single vCenter Server with local vCenter Single Sign-On in Basic deployment mode" and "Multiple vCenter Servers in a single location with one vCenter Single Sign-On server."

vCenter Single Sign-On Components

vCenter Single Sign-On includes the Security Token Service (STS), an administration server, and vCenter Lookup Service, as well as the VMware Directory Service (vmdir).

The components are deployed as part of installation.

STS (Security Token Service)

STS certificates enable a user who has logged on through vCenter Single Sign-On to use any vCenter service that vCenter Single Sign-On supports without authenticating to each one. The STS service issues Security Assertion Markup Language (SAML) tokens. These security tokens represent the identity of a user in one of the identity source types supported by vCenter Single Sign-On.

Administration server

The administration server allows users with administrator privileges to vCenter Single Sign-On to configure the vCenter Single Sign-On server and manage users and groups from the vSphere Web Client. Initially, only the user administrator@vsphere.local has these privileges.

vCenter Lookup Service

vCenter Lookup Service contains topology information about the vSphere infrastructure, enabling vSphere components to connect to each other securely. Unless you are using Simple Install, you are prompted for the Lookup Service URL when you install other vSphere components. For example, the Inventory Service and the vCenter Server installers ask for the Lookup Service URL and then contact the Lookup Service to find vCenter Single Sign-On. After installation, the Inventory Service and vCenter Server system are registered in vCenter Lookup Service so other vSphere components, like the vSphere Web Client, can find them.

VMware Directory Service

Directory service associated with the vsphere.local domain. This service is a multi-tenanted, multi-mastered directory service that makes an LDAP directory available on port 11711. In multisite mode, an update of VMware Directory Service content in one VMware Directory Service instance results in the automatic update of the VMware Directory Service instances associated with all other vCenter Single Sign-On nodes.

Setting the vCenter Server Administrator User

The way you set the vCenter Server administrator user depends on your vCenter Single Sign On deployment.

In vSphere versions before vSphere 5.1, vCenter Server administrators are the users that belong to the local operating system administrators group.

In vSphere 5.1.x and 5.5, when you install vCenter Server, you must provide the default (initial) vCenter Server administrator user or group. For deployments where vCenter Server and vCenter Single Sign-On are on the same host machine, you can designate the local operating system group Administrators as vCenter Server administrative users. This option is the default. This behavior is unchanged from vCenter Server 5.0.

For larger installations, where vCenter Single Sign-On and vCenter Server are deployed on different hosts, you cannot preserve the same behavior as in vCenter Server 5.0. Instead, assign the vCenter Server administrator role to a user or group from an identity source that is registered in the vCenter Single Sign-On server: Active Directory, OpenLDAP, or the system identity source.

Authenticating to the vCenter Server Environment

In vCenter Server versions 5.1 and later, users authenticate through vCenter Single Sign-On.

In vCenter Server versions earlier than vCenter Server 5.1, when a user connects to vCenter Server, vCenter Server authenticates the user by validating the user against an Active Directory domain or the list of local operating system users.

The user administrator@vsphere.local has vCenter Single Sign-On administrator privileges by default. When logged in to the vCenter Single Sign-On server from the vSphere Web Client, the administrator@vsphere.local user can assign vCenter Single Sign-On administrator privileges to other users. These users might be different from the users that administer vCenter Server.

Users can log in to vCenter Server with the vSphere Web Client. Users authenticate to vCenter Single Sign-On. Users can view all the vCenter Server instances that the user has permissions on. After users connect to vCenter Server, no further authentication is required. The actions users can perform on objects depend on the user's vCenter Server permissions on those objects.

For more information about vCenter Single Sign-On, see *vSphere Security*.

How vCenter Single Sign-On Affects Log In Behavior

vCenter Single Sign-On log in behavior depends on the domain the user belongs to and the identity sources that you have added to vCenter Single Sign-On.

When a user logs in to a vCenter Server system from the vSphere Web Client, the login behavior depends on whether the user is in the default domain.

- Users who are in the default domain can log in with their user name and password.
- Users who are in a domain that has been added to vCenter Single Sign-On as an identity source but is not the default domain can log in to vCenter Server but must specify the domain in one of the following ways.
  - Including a domain name prefix, for example, MYDOMAIN\user1
  - Including the domain, for example, user1@mydomain.com
- Users who are in a domain that is not a vCenter Single Sign-On identity source cannot log in to vCenter Server. If the domain that you add to vCenter Single Sign-On is part of a domain hierarchy, Active Directory determines whether users of other domains in the hierarchy are authenticated or not.

After installation on a Windows system, the user administrator@vsphere.local has administrator privileges to both the vCenter Single Sign-On server and to the vCenter Server system.

After you deploy the vCenter Virtual Appliance, the user administrator@vsphere.local has administrator privileges to both the vCenter Single Sign-On server and to the vCenter Server system. The user root@localos has administrative privileges on the vCenter Single Sign-On server and can authenticate to the vCenter Server system. Assign permissions to root@localos to allow that user access to the vCenter Server system.

Identity Sources for vCenter Server with vCenter Single Sign-On

Identity sources allow you to attach one or more domains to vCenter Single Sign-On. A domain is a repository for users and groups that the vCenter Single Sign-On server can use for user authentication.

An identity source is a collection of user and group data. The user and group data is stored in Active Directory, OpenLDAP, or locally to the operating system of the machine where vCenter Single Sign-On is installed. Upon installation, every instance of vCenter Single Sign-On has the Local OS identity source identity source vpshere.local. This identity source is internal to vCenter Single Sign-On.

A vCenter Single Sign-On administrator user can create vCenter Single Sign-On users and groups.

Types of Identity Sources

vCenter Server versions earlier than version 5.1 supported Active Directory and local operating system users as user repositories. As a result, local operating system users could always authenticate to the vCenter Server system. vCenter Server version 5.1 and version 5.5 uses vCenter Single Sign-On for authentication. See the vSphere 5.1 documentation for a list of supported identity sources with vCenter Single Sign-On 5.1. vCenter Single Sign-On 5.5 supports the following types of user repositories as identity sources, but supports only one default identity source.

- Active Directory versions 2003 and later. vCenter Single Sign-On allows you to specify a single Active Directory domain as an identity source. The domain can have child domains or be a forest root domain. Shown as **Active Directory (Integrated Windows Authentication)** in the vSphere Web Client.
- Active Directory over LDAP. vCenter Single Sign-On supports multiple Active Directory over LDAP identity sources. This identity source type is included for compatibility with the vCenter Single Sign-On service included with vSphere 5.1. Shown as **Active Directory as an LDAP Server** in the vSphere Web Client.
- OpenLDAP versions 2.4 and later. vCenter Single Sign-On supports multiple OpenLDAP identity sources. Shown as **OpenLDAP** in the vSphere Web Client.
- Local operating system users. Local operating system users are local to the operating system where the vCenter Single Sign-On server is running. The local operating system identity source exists only in basic vCenter Single Sign-On server deployments and is not available in deployments with multiple vCenter Single Sign-On instances. Only one local operating system identity source is allowed. Shown as **localos** in the vSphere Web Client.
- vCenter Single Sign-On system users. Exactly one system identity source named vsphere.local is created when you install vCenter Single Sign-On. Shown as **vsphere.local** in the vSphere Web Client.

NOTE At any time, only one default domain exists. If a user from a non-default domain logs in, that user must add the domain name (*DOMAIN\user*) to authenticate successfully.

vCenter Single Sign-On identity sources are managed by vCenter Single Sign-On administrator users.

You can add identity sources to a vCenter Single Sign-On server instance. Remote identity sources are limited to Active Directory and OpenLDAP server implementations.

For more information about vCenter Single Sign-On, see *vSphere Security*.

Login Behavior

When a user logs in to a vCenter Server system from the vSphere Web Client, the login behavior depends on whether the user is in the default domain.

- Users who are in the default domain can log in with their user name and password.

- Users who are in a domain that has been added to vCenter Single Sign-On as an identity source but is not the default domain can log in to vCenter Server but must specify the domain in one of the following ways.
  - Including a domain name prefix, for example, MYDOMAIN\user1
  - Including the domain, for example, user1@mydomain.com
- Users who are in a domain that is not a vCenter Single Sign-On identity source cannot log in to vCenter Server. If the domain that you add to vCenter Single Sign-On is part of a domain hierarchy, Active Directory determines whether users of other domains in the hierarchy are authenticated or not.

vCenter Single Sign-On does not propagate permissions that result from nested groups from dissimilar identity sources. For example, if you add the Domain Administrators group to the Local Administrators group, the permissions are not propagated because Local OS and Active Directory are separate identity sources.

vCenter Server Upgrade Summary

The upgrade to vCenter Server 5.5.x affects other software components of your datacenter.

Table 3-2 summarizes the effect on your datacenter components.

Table 3-2. Upgrading vCenter Server and Related Components

Product or Component	Description
vCenter Server	Verify support for the upgrade path from your current version of vCenter Server to the version that you are upgrading to. See the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.
vCenter Server database	Verify that your database is supported for the vCenter Server version that you are upgrading to. Upgrade the database if necessary. See the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php. NOTE The version 5.5.x vCenter Server Appliance uses PostgreSQL for the embedded database. For external databases, the vCenter Server Appliance supports only Oracle databases, in the same versions shown in the VMware Product Interoperability Matrix for the version of vCenter Server that you are upgrading to.
vSphere Web Client	Verify that your vSphere Web Client works with the vCenter Server version that you are upgrading to. For best performance and compatibility, upgrade your vSphere Web Client to the same version as your vCenter Server. See the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.
ESX and ESXi hosts	Verify that your ESX or ESXi host works with the vCenter Server version that you are upgrading to. Upgrade if necessary. See the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.
VMFS2 volumes	Supported as read-only (deprecated).
VMFS3 volumes	No change.
VMDK2 virtual disk	Not supported.
VMDK3 virtual disk	Not supported.
Virtual machines	Upgrade options depend on your current version. See Chapter 8, "Upgrading Virtual Machines and VMware Tools," on page 215.
VMware Tools	Upgrade options depend on your current version. See the information about upgrading VMware Tools in Chapter 8, "Upgrading Virtual Machines and VMware Tools," on page 215.
Auto Deploy 5.0.x, 5.1 x, and 5.5.0	To ensure compatibility and best performance, when you upgrade to vCenter Server 5.5.x, Auto Deploy to the same version.

Required Information for Installing or Upgrading vCenter Single Sign-On, Inventory Service, vCenter Server, and the vSphere Web Client

Prepare for the vCenter Server installation by recording the values that vCenter Server and related components require.

The vCenter Single Sign-On, vSphere Web Client, vCenter Inventory Service, and vCenter Server installation wizards prompt you for the installation or upgrade information. Keep a record of the values entered, in case you must reinstall vCenter Server. You can print this topic as a worksheet to record the information that you need for the installation or upgrade of vCenter Single Sign-On, the vSphere Web Client, Inventory Service, and vCenter Server.

The following tables list the required information for installing or upgrading vCenter Single Sign-On, the vSphere Web Client, vCenter Inventory Service, and vCenter Server.

- Table 3-3.
- Table 3-4.
- Table 3-5.
- Table 3-6.

NOTE Depending on the type of installation or upgrade you are doing, some entries might not be required.

Table 3-3. Information Required for vCenter Single Sign-On Installation.

Required Information	Default	Your Entry
Setup Language. This selection controls the language only for the installer.	English	
vCenter Single Sign-On HTTPS port.	7444	
vCenter Single Sign-On deployment type. Choose from the following options: ■ vCenter Single Sign-On for your first vCenter Server. Select this option to create a new vCenter Single Sign-On server, which will become the first vCenter Single Sign-On server in a new domain.. ■ vCenter Single Sign-On for an additional vCenter Server in an existing site. Select this option to create an additional vCenter Single Sign-On server that replicates information from an existing vCenter Single Sign-On server in the domain. ■ vCenter Single Sign-On for an additional vCenter Server with a new site. Select this option to create an additional vCenter Single Sign-On server that replicates information from an existing vCenter Single Sign-On server in a different site.		
Domain name.	vsphere.local	You cannot change the domain name from the default during installation.
User name.	administrator@vsphere.local	You cannot change the user name from the default during installation.

Table 3-3. Information Required for vCenter Single Sign-On Installation. (Continued)

Required Information	Default	Your Entry
Password for the vCenter Single Sign-On administrator account in the default domain. You must use the same vCenter Single Sign-On password name when you install or upgrade vCenter Single Sign-On, Inventory Service, vCenter Server, and the vSphere Web Client. IMPORTANT Be sure to record the password. If you need to restore the vCenter Single Sign-On configuration from a backup, the restore process requires the password you enter for the original vCenter Single Sign-On installation, even if you change the password later. By default, the password must have at least eight characters, at least one lowercase character, one uppercase character, one number, and one special character. See the *vSphere Security* documentation for information about changing the password policy. The following characters are not supported in passwords: non-ASCII characters, semicolon (;), double quotation mark ("), single quotation mark ('), circumflex (^), and backslash (\).		
Site name. Your name for the vCenter Single Sign-On site.		
Partner host name. Required only if you are installing additional vCenter Single Sign-On servers. The partner host name is the DNS name of the existing vCenter Single Sign-On server to replicate from.		

Table 3-4. Information Required for the vSphere Web Client Installation

Required Information	Default	Your Entry
Setup Language. This selection controls the language only for the installer.	English	
Destination folder. The folder to install the vSphere Web Client in. The installation path cannot contain the following characters: non-ASCII characters, commas (,), periods (.), exclamation points (!), pound signs (#), at signs (@), or percentage signs (%). If 8.3 name creation is disabled on the host machine, do not install the vSphere Web Client in a directory that does not have an 8.3 short name or has a name that contains spaces. This situation will make the vSphere Web Client inaccessible.	`C:\Program Files\VMware\Infrastructure`	
vSphere Web Client HTTP port.	9090	
vSphere Web Client HTTPS port.	9443	
vCenter Single Sign-On administrator user name. The entry is case sensitive, and must match the administrator user name you enter when you install vCenter Single Sign-On	administrator@vsphere.local	

Table 3-4. Information Required for the vSphere Web Client Installation (Continued)

Required Information	Default	Your Entry
Password for the vCenter Single Sign-On administrator account in the default domain. You must use the same vCenter Single Sign-On password when you install or upgrade vCenter Single Sign-On, Inventory Service, vCenter Server, and the vSphere Web Client. IMPORTANT Be sure to record the password. If you need to restore the vCenter Single Sign-On configuration from a backup, the restore process requires the password you enter for the original vCenter Single Sign-On installation, even if you change the password later.		
Lookup Service URL. The Lookup Service URL takes the form https://*SSO_host_FQDN_or_IP*:7444/lookupservice/sdk, where 7444 is the default vCenter Single Sign-On HTTPS port number. This entry must match the URL you enter when you install vCenter Inventory Service.		

Table 3-5. Information Required for vCenter Inventory Service Installation or Upgrade

Required Information	Default	Your Entry
Setup Language. This selection controls the language only for the installer.	English	
Destination folder. The folder to install Inventory Service in. The installation path cannot contain the following characters: non-ASCII characters, commas (,), periods (.), exclamation points (!), pound signs (#), at signs (@), or percentage signs (%).	`C:\Program Files\VMware\Infrastructure`	
Fully Qualified Domain Name. The FQDN for the Inventory Service local system.		
vCenter Inventory Service HTTPS port.	10443	
vCenter Inventory Service management port.	10109	
vCenter Inventory Service Linked Mode communication port.	10111	
Inventory size. The inventory size of your vCenter Server deployment: ■ Small (less than 100 hosts or 1000 virtual machines. ■ Medium (100-400 hosts or 1000-4000 virtual machines. ■ Large (more than 400 hosts or 4000 virtual machines. This setting determines the maximum JVM heap settings for VMware VirtualCenter Management Webservices (Tomcat), Inventory Service, and Profile-Driven Storage Service. You can adjust this setting after installation if the number of hosts in your environment changes. See the recommendations in "Hardware Requirements for vCenter Server, the vSphere Web Client, vCenter Inventory Service, and vCenter Single Sign-On," on page 17.		

See "Required Ports for vCenter Server," on page 23.

Table 3-5. Information Required for vCenter Inventory Service Installation or Upgrade (Continued)

Required Information	Default	Your Entry
User name for the vCenter Single Sign-On administrator user account. You must use the same vCenter Single Sign-On user name and password name when you install vCenter Single Sign-On, and install or upgrade Inventory Service, vCenter Server, and the vSphere Web Client.	administrator	
Lookup Service URL. The Lookup Service URL takes the form https://*SSO_host_FQDN_or_IP*:7444/lookupservice/sdk, where 7444 is the default vCenter Single Sign-On HTTPS port number. If you enter a different port number when you install vCenter Single Sign-On, use that port number.		

Table 3-6. Information Required for vCenter Server Installation or Upgrade

Required Information	Default	Your Entry
Setup Language. This selection controls the language only for the installer.	English	
vCenter Server license key. If you omit the license key, vCenter Server is installed in evaluation mode. After you install vCenter Server, you can enter the vCenter Server license in the vSphere Web Client.		
Data source name (DSN). Required if you use an existing database. Not required if you are using the bundled Microsoft SQL Server 2008 Express database. Leading and trailing spaces are not supported. Remove spaces from the beginning or end of the DSN.		
Database user name.	Required to use an existing database. Not required if you are using the bundled database. Non-ASCII characters are not supported.	
Database password.		
JDBC URL for database. Required if you use an existing database. The vCenter Server installer should generate and validate the JDBC URL for the vCenter Server database. If the installer fails to connect to the database by using the generated JDBC URL, the installer prompts you to specify the JDBC URL. The format of the JDBC URL depends on the database that you are using. See "JDBC URL Formats for the vCenter Server Database," on page 55.v		
vCenter Server Service account information. Can be the Microsoft Windows system account or a user-specified account. Use a user-specified account if you plan to use Microsoft Windows authentication for SQL Server.	Microsoft Windows system account	
Fully qualified domain name (FQDN) for the vCenter Server machine The FQDN of the system that you are installing vCenter Server on. The vCenter Server installer checks that the FQDN is resolvable. If not, a warning message appears. Change the entry to a resolvable FQDN. You must enter the FQDN, not the IP address.		
Standalone or join group. Join a Linked Mode group to enable the vSphere Web Client to view, search, and manage data across multiple vCenter Server systems.	Standalone	

Table 3-6. Information Required for vCenter Server Installation or Upgrade (Continued)

Required Information		Default	Your Entry
Fully qualified domain name of Directory Services for the vCenter Server group. The FQDN of a remote instance of vCenter Server. Required if this instance of vCenter Server is joining a group. The local and remote instances will be members of a Linked Mode group.			
LDAP port for the Directory Services for the remote vCenter Server instance. The LDAP port of the remote instance. Required if this instance of vCenter Server is joining a Linked Mode group. See "Required Ports for vCenter Server," on page 23.		389	
vCenter Server HTTPS port.	See "Required Ports for vCenter Server," on page 23.	443	
vCenter Server HTTP port.		80	
Heartbeat port (UDP) used for sending data to ESX/ESXi hosts.		902	
VMware VirtualCenter Management Web Services HTTP port		8080	
VMware VirtualCenter Management Web Services HTTPS port.		8443	
Web Services change service notification port.		60099	
LDAP port for the Directory Services for the local vCenter Server instance.		389	
SSL port for the Directory Services for the local vCenter Server instance.		636	
Ephemeral ports. Select **Increase the number of available ephemeral ports** if your vCenter Server manages hosts on which you will power on more than 2000 virtual machines simultaneously. This option prevents the pool of available ephemeral ports from being exhausted.			

Table 3-6. Information Required for vCenter Server Installation or Upgrade (Continued)

Required Information	Default	Your Entry
Inventory size. The inventory size of your vCenter Server deployment: ■ Small (less than 100 hosts or 1000 virtual machines. ■ Medium (100-400 hosts or 1000-4000 virtual machines. ■ Large (more than 400 hosts or 4000 virtual machines. This setting determines the maximum JVM heap settings for VMware VirtualCenter Management Webservices (Tomcat), Inventory Service, and Profile-Driven Storage Service. You can adjust this setting after installation if the number of hosts in your environment changes. See the recommendations in "Hardware Requirements for vCenter Server, the vSphere Web Client, vCenter Inventory Service, and vCenter Single Sign-On," on page 17.		
User name for the vCenter Single Sign-On administrator user account.	You must use the same vCenter Single Sign-On user name and password name when you install vCenter Single Sign-On, and install or upgrade Inventory Service, vCenter Server, and the vSphere Web Client.	administrator
Password for the vCenter Single Sign-On administrator user account.		
Lookup Service URL. The Lookup Service URL takes the form https://*SSO_host_FQDN_or_IP*:7444/lookupservice/sdk, where 7444 is the default vCenter Single Sign-On HTTPS port number. If you enter a different port number when you install vCenter Single Sign-On, use that port number.		
Inventory Service URL. The inventory Service URL takes the form https://*Inventory_Service_host_FQDN_or_IP*:10443. 10443 is the default Inventory Service HTTPS port number. If you enter a different port number when you install Inventory Service, use that port number.		
Destination folder. The folder to install vCenter Server in. The installation path cannot contain the following characters: non-ASCII characters, commas (,), periods (.), exclamation points (!), pound signs (#), at signs (@), or percentage signs (%).	`C:\Program Files\VMware\Infrastructure`	

Best Practices for vCenter Server Upgrades

When you upgrade vCenter Server, you must understand and follow the best practices process for a successful upgrade.

To ensure that each upgrade is successful, follow these best practices:

1 Make sure that you understand the vCenter Server upgrade process, the effect of that process on your existing deployment, and the preparation required for the upgrade.

   - If your vSphere system includes VMware solutions or plug-ins, make sure they are compatible with the vCenter Server version that you are upgrading to. See the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.
   - Read all the subtopics in Chapter 3, "Preparing for the Upgrade to vCenter Server," on page 31.

- Read the VMware vSphere Release Notes for known installation issues.
- If your vSphere installation is in a VMware View environment, see "Upgrading vSphere Components Separately in a Horizon View Environment," on page 220.

2 Prepare your system for the upgrade.

- Make sure your system meets requirements for the vCenter Server version that you are upgrading to. See Chapter 2, "System Requirements," on page 13 and the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.
- Verify that your existing database is supported for the vCenter Server version that you are upgrading to. See the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.
- Make sure that your vCenter Server database is prepared and permissions are correctly set. See the information about preparing vCenter Server databases in the *vSphere Installation and Setup* documentation.
- Review the prerequisites for the upgrade. See "Prerequisites for the vCenter Server Upgrade," on page 48.

3 Back up your vCenter Server databases and SSL certificates

- Make a full backup of the vCenter Server database and the vCenter Inventory Service database. For the vCenter Server database, see the vendor documentation for your vCenter Server database type. For the Inventory Service database, see the topics "Back Up the Inventory Service Database on Windows" and "Back Up the Inventory Service Database on Linux" in the *vSphere Installation and Setup* documentation.
- Back up the SSL certificates that are on the vCenter Server system before you upgrade to vCenter Server 5.5. The default location of the SSL certificates is `%allusersprofile%\Application Data\VMware\VMware VirtualCenter`.

4 Stop the VMware VirtualCenter Server service.

5 Run the vCenter Host Agent Pre-Upgrade Checker, and resolve any issues. See "Run the vCenter Host Agent Pre-Upgrade Checker," on page 57.

6 Make sure that no processes are running that conflict with the ports that vCenter Server uses. See "Required Ports for vCenter Server," on page 23.

7 Upgrade vCenter Server and required components.

See the appropriate procedure for your existing vCenter Server deployment:

- "Use Simple Install to Upgrade vCenter Server and Required Components," on page 65
- "Use Custom Install to Upgrade a Basic vCenter Single Sign-On Deployment of Version 5.1.x vCenter Server and Required Components," on page 78
- "Use Custom Install to Upgrade vCenter Server from a Version 5.1.x High Availability vCenter Single Sign-On Deployment," on page 84
- "Use Custom Install to Upgrade vCenter Server from a Version 5.1.x Multisite vCenter Single Sign-On Deployment," on page 93

8 Configure new vSphere 5.5 licenses.

9 Review the topics in Chapter 5, "After You Upgrade vCenter Server," on page 127 for postupgrade requirements and options.

Prerequisites for the vCenter Server Upgrade

Before you begin the upgrade to vCenter Server, make sure you prepare the vCenter Server system and the database.

Prerequisites for Understanding and Preparing for the Upgrade Process

- vCenter Server 5.5 requires vCenter Single Sign-On and Inventory Service. Install or update these components in this order: vCenter Single Sign-On, the vSphere Web Client, Inventory Service, and vCenter Server. Review the topics in the section "How vCenter Single Sign-On Affects vCenter Server Upgrades," on page 32
- Review the release notes for known issues or special installation notes.
- Gather the information that is required to complete the installation wizard. See "Required Information for Installing or Upgrading vCenter Single Sign-On, Inventory Service, vCenter Server, and the vSphere Web Client," on page 41.
- Download the vCenter Server installer from the VMware Web site.

System Prerequisites

- Verify that your system meets the requirements listed in "Hardware Requirements for vCenter Server, the vSphere Web Client, vCenter Inventory Service, and vCenter Single Sign-On," on page 17 and "vCenter Server Software Requirements," on page 22, and that the required ports are open, as discussed in "Required Ports for vCenter Server," on page 23.
- If your vSphere system includes VMware solutions or plug-ins, make sure they are compatible with the vCenter Server version that you are upgrading to. See the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.
- Before you upgrade any vCenter Server that belongs to a Linked Mode group, remove it from the Linked Mode group. Upgrading vCenter Servers that are members of a Linked Mode group can cause the upgrade to fail, and can leave vCenter Servers in an unusable state. After you upgrade all members of a Linked Mode group to version 5.5, you can rejoin them.
- If you do not intend to use evaluation mode, make sure that you have valid license keys for all purchased functionality. License keys from vSphere versions prior to version 5.0 are not supported in vCenter Server 5.x. If you do not have the license key, you can install in evaluation mode and use the vSphere Web Client to enter the license key later.
- Close all instances of the vSphere Web Client.
- Verify that the system on which you are upgrading vCenter Server is not an Active Directory primary or backup domain controller.
- Either remove any ESX Server 2.x or 3.x hosts from the vCenter Server inventory or upgrade these hosts to version 4.0 or later.
- Update any ESX/ESXi 4.1 hosts to version 4.1 Update 1 or later. See Knowledge Base article 2009586.
- Before you install or upgrade any vSphere product, synchronize the clocks of all machines on the vSphere network. See "Synchronizing Clocks on the vSphere Network," on page 53.
- Verify that the fully qualified domain name (FQDN) of the system where you will upgrade vCenter Server is resolvable. To check that the FQDN is resolvable, type **`nslookup`** ***`your_vCenter_Server_fqdn`*** at a command line prompt. If the FQDN is resolvable, the **`nslookup`** command returns the IP and name of the domain controller machine.
- Run the vCenter Host Agent Pre-Upgrade Checker.

- The installation path of the previous version of vCenter Server must be compatible with the installation requirements for Microsoft Active Directory Application Mode (ADAM/AD LDS). The installation path cannot contain any of the following characters: non-ASCII characters, commas (,), periods (.), exclamation points (!), pound signs (#), at signs (@), or percentage signs (%). If your previous version of vCenter Server does not meet this requirement, you must perform a clean installation of vCenter Server.
- Back up the SSL certificates that are on the vCenter Server system before you upgrade to vCenter Server 5.5. The default location of the SSL certificates is `%allusersprofile%\Application Data\VMware\VMware VirtualCenter`.
- Make sure that SSL certificate checking is enabled for all vSphere HA clusters. If certificate checking is not enabled when you upgrade, HA will fail to configure on the hosts. Select **Administration > vCenter Server Settings > SSL Settings > vCenter requires verified host SSL certificates**. Follow the instructions to verify each host SSL certificate and click **OK**.
- If the vCenter Server 4.x environment that you are upgrading includes Guided Consolidation 4.x, uninstall Guided Consolidation before upgrading to vCenter Server 5.5.
- Before the vCenter Server installation, in the Administrative Tools control panel of the vCenter Single Sign-On instance that you will register vCenter Server to, verify that the following services are started: VMware Certificate Service, VMware Directory service , VMware Identity Manager Service, VMware KDC service, and tcruntime-C-ProgramData-VMware-cis-runtime-VMwareSTSService.
- You must log in as a member of the Administrators group on the host machine, with a user name that does not contain any non-ASCII characters.

Network Prerequisites

- Verify that DNS reverse lookup returns a fully qualified domain name when queried with the IP address of the vCenter Server. When you upgrade vCenter Server, the installation of the web server component that supports the vSphere Web Client fails if the installer cannot look up the fully qualified domain name of the vCenter Server from its IP address. Reverse lookup is implemented using PTR records. To create a PTR record, see the documentation for your vCenter Server host operating system.
- If you use DHCP instead of a manually assigned (static) IP address for vCenter Server, make sure that the vCenter Server computer name is updated in the domain name service (DNS). Test this is by pinging the computer name. For example, if the computer name is `host-1.company.com`, run the following command in the Windows command prompt:

  ```
  ping host-1.company.com
  ```

  If you can ping the computer name, the name is updated in DNS.
- Ensure that the ESXi host management interface has a valid DNS resolution from the vCenter Server and all vSphere Web Clients. Ensure that the vCenter Server has a valid DNS resolution from all ESXi hosts and all vSphere Web Clients.
- If you will use Active Directory as an identity source, verify that it is set up correctly. The DNS of the vCenter Single Sign-On Server host machine must contain both lookup and reverse lookup entries for the domain controller of the Active Directory. For example, pinging *mycompany.com* should return the domain controller IP address for *mycompany*. Similarly, the `ping -a` command for that IP address should return the domain controller hostname. Avoid trying to correct name resolution issues by editing the hosts file. Instead, make sure that the DNS server is correctly set up. For more information about configuring Active Directory, see the Microsoft Web site. Also, the system clock of the vCenter Single Sign-On Server host machine must be synchronized with the clock of the domain controller.

Prerequisites for All vCenter Server Databases

- If your database server is not supported by vCenter Server, perform a database upgrade to a supported version or import your database into a supported version. See "Supported Database Upgrades," on page 53.
- Perform a complete backup of the vCenter Server database before you begin the upgrade.

  If you choose to remove the DBO role, you can migrate all objects in the DBO schema to a custom schema. See the VMware knowledge base article at http://kb.vmware.com/kb/1036331.
- You must have login credentials, the database name, and the database server name that will be used by the vCenter Server database. The database server name is typically the ODBC System database source name (DSN) connection name for the vCenter Server database.
- Review "Supported Database Upgrades," on page 53.

Prerequisites for Microsoft SQL Databases

- To use a newly supported Microsoft SQL database, such as Microsoft SQL 2008, you do not need to perform a clean installation of vCenter Server if your existing database is also Microsoft SQL Server. For example, you can upgrade a Microsoft SQL Server 2000 database to Microsoft SQL Server 2008 and then upgrade vCenter Server 4.0 or higher to vCenter Server 5.5. When you migrate the database from Microsoft SQL Server 2000 to Microsoft SQL Server 2008 or higher, set the compatibility level of the database to 90.
- JDK 1.6 must be installed on the vCenter Server machine. In addition, `sqljdbc4.jar` must be added to the CLASSPATH variable on the machine where vCenter Server is to be upgraded. If it is not installed on your system, the vCenter Server installer installs it. The JDK 1.6 installation might require Internet connectivity.
- Your system DSN must be using the SQL Native Client driver.
- If you choose to remove the DBO role and migrate all objects in the DBO schema to a custom schema, as described in the VMware knowledge base article at http://kb.vmware.com/kb/1036331, grant the following permissions to the vCenter user in the vCenter database:

  ```
  GRANT ALTER ON SCHEMA :: <schema> to <user>;
  GRANT REFERENCES ON SCHEMA :: <schema> to <user>;
  GRANT INSERT ON SCHEMA :: <schema>  to <user>;
  GRANT CREATE TABLE to <user>;
  GRANT CREATE VIEW to <user>;
  GRANT CREATE Procedure to <user>;
  ```

  Grant the following permissions to the user in the MSDB database:

  ```
  GRANT SELECT on msdb.dbo.syscategories to <user>;
  GRANT SELECT on msdb.dbo.sysjobsteps to <user>;
  GRANT SELECT ON msdb.dbo.sysjobs to <user>;
  GRANT EXECUTE ON msdb.dbo.sp_add_job TO <user>;
  GRANT EXECUTE ON msdb.dbo.sp_delete_job TO <user>;
  GRANT EXECUTE ON msdb.dbo.sp_add_jobstep TO <user>;
  GRANT EXECUTE ON msdb.dbo.sp_update_job TO <user>;
  GRANT EXECUTE ON msdb.dbo.sp_add_category TO <user>;
  GRANT EXECUTE ON msdb.dbo.sp_add_jobserver TO <user>;
  GRANT EXECUTE ON msdb.dbo.sp_add_jobschedule TO <user>;
  ```

Prerequisites for Oracle Databases

- To use a newly supported Oracle database, such as Oracle 11g, you do not need to perform a clean installation of vCenter Server if your existing database is also Oracle. For example, you can upgrade your existing Oracle 9i database to Oracle 11g and then upgrade vCenter Server 4.x to vCenter Server 5.5.
- The JDBC driver file must be included in the CLASSPATH variable.
- Either assign the DBA role or grant the following permissions to the user:

```
grant connect to <user>
grant resource to <user>
grant create view to <user>
grant create any sequence to <user>
grant create any table to <user>
grant create materialized view to <user>
grant execute on dbms_job to <user>
grant execute on dbms_lock to <user>
grant unlimited tablespace to <user> # To ensure sufficient space
```

  After the upgrade is complete, you can optionally remove the following permissions from the user profile: **create any sequence** and **create any table**.

  By default, the **RESOURCE** role has the **CREATE PROCEDURE**, **CREATE TABLE**, and **CREATE SEQUENCE** privileges assigned. If the **RESOURCE** role lacks these privileges, grant them to the vCenter Server database user.

vCenter Server Database Configuration Notes

After you choose a supported database type, make sure you understand any special configuration requirements.

Table 3-7 is not a complete list of databases supported with vCenter Server. For information about specific database versions and service pack configurations supported with vCenter Server, see the VMware Product Interoperability Matrixes. This topic is intended only to provide special database configuration notes not listed in the Product Interoperability Matrixes.

NOTE vCenter Update Manager also requires a database. VMware recommends that you use separate databases for vCenter Server and vCenter Update Manager.

---

vCenter Server databases require a UTF code set.

See also "Supported Database Upgrades," on page 53.

Table 3-7. Configuration Notes for Databases Supported with vCenter Server

Database Type	Configuration Notes
Microsoft SQL Server 2008 R2 Express	Bundled database that you can use for small deployments of up to 5 hosts and 50 virtual machines. SQL Server Collation Model: SQL_Latin1_General_CP1_CI_AS. ODBC System DSN minimum version: SQL Native Client 10.0 (version 2009.100.4000.00), which you can obtain as a free download from the microsoft.com Download Center. You cannot install the bundled database during an upgrade to vCenter Server. To use the bundled database, Microsoft SQL Server 2008 R2 Express must be already installed or you must perform a clean installation of vCenter Server. NOTE This database is not supported for the vCenter Server Appliance.
Microsoft SQL Server 2008	Ensure that the machine has a valid ODBC DSN entry. SQL Server Collation Model: SQL_Latin1_General_CP1_CI_AS. ODBC System DSN minimum version: SQL Native Client 10.0 (version 2009.100.4000.00), which you can obtain as a free download from the microsoft.com Download Center. NOTE This database is not supported for the vCenter Server Appliance.
Microsoft SQL Server 2012 SP1	Ensure that the machine has a valid ODBC DSN entry.
Oracle 11g and 12c	Ensure that the machine has a valid ODBC DSN entry. After you complete the vCenter Server installation, take the following steps: ■ Apply the latest patch to the Oracle client and server. ■ Copy the Oracle JDBC driver (ojdbc14.jar or ojdbc5.jar) to the vCenter Server installation directory, in the `tomcat\lib` subdirectory: *`vCenter install location`*`\Infrastructure\tomcat\lib`. ■ In the Services section of the Windows Administrative Tools control panel, restart the VMware VirtualCenter Management Webservices service. The vCenter Server installer attempts to copy the Oracle JDBC driver from the Oracle client location to the vCenter Server installation directory. If the Oracle JDBC driver is not found in the Oracle client location, the vCenter Server installer prompts you to copy the file manually. You can download the file from the oracle.com Web site.

Upgrading to vCenter Server on a Different Machine

Instead of performing an in-place upgrade to vCenter Server, you might want to use a different machine for your upgrade. Because vCenter Server 5.x requires a 64-bit platform, you cannot upgrade from a version of vCenter Server installed on a 32-bit platform.

The vCenter Server 5.0 installation media include a data migration tool. When you upgrade to version 5.0, you can use this tool to migrate configuration information such as port settings, SSL certificates, and license information from your existing vCenter Server host. This data migration tool is not supported for vCenter Server versions 5.1 and later. You cannot directly migrate an existing vCenter Server to a different machine during an upgrade to version 5.1.x or 5.5. You can migrate an existing vCenter Server to a different machine during an upgrade to version 5.0, and then perform an in-place upgrade from version 5.0 to version 5.1.x or 5.5. See the version 5.0 *vSphere Upgrade* documentation.

Supported Database Upgrades

When you upgrade to vCenter Server 5.5, make sure that the upgraded version supports your database.

For a list of the specific database versions supported for the version of vCenter Server that you are upgrading to, see the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

NOTE The version 5.5 vCenter Server Appliance uses a PostgreSQL for the embedded database. For external databases, the vCenter Server Appliance supports only Oracle databases, in the same versions shown in the VMware Product Interoperability Matrix for the version of vCenter Server that you are upgrading to.

Confirm That vCenter Server Can Communicate with the Local Database

If your database is located on the same machine on which vCenter Server will be installed, and you have changed the name of this machine, make sure the vCenter Server DSN is configured to communicate with the new name of the machine.

Changing the vCenter Server computer name impacts database communication if the database server is on the same computer with vCenter Server. If you changed the machine name, you can verify that communication remains intact.

The name change has no effect on communication with remote databases. You can skip this procedure if your database is remote.

Check with your database administrator or the database vendor to make sure all components of the database are working after you rename the server.

Prerequisites

- Make sure the database server is running.
- Make sure that the vCenter Server computer name is updated in the domain name service (DNS).

Procedure

1 Update the data source information, as needed.

2 Ping the computer name to test this connection.

For example, if the computer name is `host-1.company.com`, run the following command in the Windows command prompt:

```
ping host-1.company.com
```

If you can ping the computer name, the name is updated in DNS.

Synchronizing Clocks on the vSphere Network

Before you install vCenter Single Sign-On, install the vSphere Web Client, or deploy the vCenter Server Appliance, make sure that all machines on the vSphere network have their clocks synchronized.

If the clocks on vCenter Server network machines are not synchronized, SSL certificates, which are time-sensitive, might not be recognized as valid in communications between network machines. Unsynchronized clocks can result in authentication problems, which can cause the vSphere Web Client installation to fail or prevent the vCenter Server Appliance vpxd service from starting.

Make sure that any Windows host on which a vCenter component runs is synchronized with the NTP server. See the Knowledge Base article Timekeeping best practices for Windows, including NTP.

Synchronize ESX and ESXi Clocks with a Network Time Server

Before you install vCenter Single Sign-On, the vSphere Web Client, or the vCenter Server appliance, make sure all machines on the vSphere network have their clocks synchronized.

Procedure

1 From the vSphere Web Client, connect to the vCenter Server.

2 Select the host in the inventory.

3 Select the **Manage** tab.

4 Select **Settings**.

5 In the System section, select **Time Configuration**.

6 Click **Edit** and set up the NTP server.

   a Select **Use Network Time Protocol (Enable NTP client)**.

   b Set the NTP Service Startup Policy.

   c Enter the IP addresses of the NTP servers to synchronize with.

   d Click **Start** or **Restart** in the NTP Service Status section.

7 Click **OK**.

   The host synchronizes with the NTP server.

Synchronize the vCenter Server Appliance Clock with an NTP Server

Before you deploy the vCenter Server Appliance, make sure all machines on the network have their clocks synchronized. Unsynchronized clocks can cause installation and authentication errors.

On systems that are joined to a Windows domain, the vCenter Server Appliance clock is synchronized automatically with the domain controller. On other systems, you can enable synchronizing the clock through VMware Tools. As an alternative, you can use this procedure.

Procedure

1 Open a Web browser and navigate to the vCenter Server Appliance Management Interface (https://*vCenter-Appliance-IP-Address*:5480/).

2 Log in as root.

3 From the vCenter Server tab, select the Time subtab.

4 Select one or more of the available options.

Option	Description
No synchronization	Does not perform synchronization.
NTP synchronization	Select this option and specify one or more NTP servers to configure the appliance to synchronize with an NTP server directly.
VMware Tools synchronization	Select this option to synchronize all virtual machines.
Active Directory synchronization	This option becomes available only if you add the appliance to an Active Directory domain. If you select this option, none of the other options is available.

5 Click **Save Settings**.

The vCenter Server Appliance clock is synchronized with the NTP server.

JDBC URL Formats for the vCenter Server Database

The vCenter Server installer generates and validates the JDBC URL for the vCenter Server database. If the installer fails to connect to the database using the generated JDBC URL, the installer will prompt you to specify the JDBC URL.

JDBC URL Note for All Databases

NOTE The domain name cannot contain the exclamation point character (!). Java interprets the exclamation point as a jar file separator.

JDBC URL Formats for Microsoft SQL Server Databases

For Microsoft SQL Server databases, you can use the following example JDBC URLs as a model:

- Connect to default (unnamed) SQL Server instance by host name:

  jdbc:sqlserver://*host*;databaseName=*database*

- Connect to named instance by host name and instance name:

  jdbc:sqlserver://*host*;instanceName=*instance*;databaseName=*database*

- Connect to SQL Server by host name and port:

  jdbc:sqlserver://*host*:*port*;databaseName=*database*

- Connect by port:

  jdbc:sqlserver://localhost:1422;databaseName\=VIM_VCDB (user name, password, and database type to be passed separately)

- Connect to local server with integrated security:

  jdbc:sqlserver://localhost\\SQLEXP_VIM;databaseName=VIM_VCDB;integratedSecurity=true

- Connect to local server without integrated security:

  jdbc:sqlserver://localhost\\SQLEXP_VIM;databaseName\=VIM_VCDB (user name, password, and database type to be passed separately)

VMware vCenter Server JDBC configuration for Microsoft SQL Server might not work by default with direct IPv6 addresses. You must use one of the following forms:

- Use the host name form for a standard Type-4 JDBC URL (recommended):

  jdbc:sqlserver://*database-fully-qualified-host-name*:*port*

- Use direct IPv6 address format:

  jdbc:sqlserver://;serverName=[*IPv6-address*]

For more information about JDBC URL formatting for MS SQL databases, including port and instance configuration options, see the msdn.microsoft.com Web site. At the time of this topic's publication, the information was available at http://msdn.microsoft.com/en-us/library/ms378428.aspx.

JDBC URL Formats for Oracle Databases

For Oracle databases, you can use the following example JDBC URLs as a model:

- This format requires host name and address, port (default 1521) and service name (for example, "oracle.world"):

  jdbc:oracle:thin:@*host*:*port*/*service*

- This format requires host name and address, port (default 1521) and SID (for example, "ORCL"):

  jdbc:oracle:thin:@*host*:*port*:*SID*

- This format is for a fully configured Oracle client with Oracle Net, which is useful for non-TCP configuration or Oracle RAC (real application clusters):

  jdbc:oracle:thin:@*tnsname*

- The following example is for an Oracle RAC with a thin driver, without the full Oracle client installed:

  jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=rac1-vip)(PORT=1521))
  (ADDRESS=(PROTOCOL=TCP)(HOST=rac2-vip)(PORT=1521))(LOAD_BALANCE=yes)(FAILOVER=ON)
  (CONNECT_DATA=(SERVER=DEDICATED)(SERVICE_NAME=RAC.DBTEAM)(FAILOVER_MODE=(BACKUP=rac1)
  (TYPE=SELECT)(METHOD=BASIC)))))

  In this example, **rac1-vip** is first node virtual IP, **rac2-vip** is second node virtual IP, **RAC.DBTEAM** is RAC DB service name, and **rac1** is name of failover node.

For more information about JDBC URL formatting for Oracle databases, see the oracle.com Web site.

DNS Load Balancing Solutions and vCenter Server Datastore Naming

vCenter Server 5.x uses different internal identifiers for datastores than earlier versions of vCenter Server. This change affects the way that you add shared NFS datastores to hosts and can affect upgrades to vCenter Server 5.x.

vCenter Server versions before version 5.0 convert datastore host names to IP addresses. For example, if you mount an NFS datastore by the name \\nfs-datastore\folder, pre-5.0 vCenter Server versions convert the name nfs-datastore to an IP address like 10.23.121.25 before storing it. The original nfs-datastore name is lost.

This conversion of host names to IP addresses causes a problem when DNS load balancing solutions are used with vCenter Server. DNS load balancing solutions themselves replicate data and appear as a single logical datastore. The load balancing happens during the datastore host name-to-IP conversion by resolving the datastore host name to different IP addresses, depending on the load. This load balancing happens outside vCenter Server and is implemented by the DNS server. In vCenter Server versions before version 5.0, features like vMotion do not work with such DNS load balancing solutions because the load balancing causes one logical datastore to appear as several datastores. vCenter Server fails to perform vMotion because it cannot recognize that what it sees as multiple datastores are actually a single logical datastore that is shared between two hosts.

To solve this problem, vCenter Server versions 5.0 and later do not convert datastore names to IP addresses when you add datastores. This enables vCenter Server to recognize a shared datastore, but only if you add the datastore to each host by the same datastore name. For example, vCenter Server does not recognize a datastore as shared between hosts in the following cases.

- The datastore is added by IP address to host1 and by *hostname* to host2.
- The datastore is added by *hostname* to host1, and by *hostname.vmware.com* to host2.

For vCenter Server to recognize a datastore as shared, you must add the datastore by the same name to every host.

Datastore Names and Upgrades to vCenter Server 5.x

In vCenter Server versions before version 5.0, vCenter Server database stores datastore paths in the old format, as IP addresses. The upgrade to vCenter Server 5.x converts these paths to the new format. If you use a DNS load balancing solution with shared datastores, before you upgrade to vCenter Server 5.x, make sure that every shared datastore is mounted on each of its hosts with the same name.

The upgrade to vCenter Server 5.x might also fail from a lack of sufficient memory if you use a DNS load balancing solution with shared datastores. In a large vCenter Server database, the conversion of datastore paths to the new format can require a large amount of memory. See the VMware Knowledge Base article at http://kb.vmware.com/kb/2015055.

About the vCenter Host Agent Pre-Upgrade Checker

The vCenter Host Agent Pre-Upgrade Checker produces a report showing known issues that might prevent a successful upgrade of the vCenter Host Agent software.

To ensure a successful upgrade to vCenter Server 5.x, you must diagnose and fix any potential problems on the managed ESX/ESXi hosts. You can run the vCenter Host Agent Pre-Upgrade Checker for in-place upgrades from vCenter Server 4.x to vCenter Server 5.x.

vCenter Host Agent runs on all managed ESX/ESXi hosts. This software coordinates actions received from vCenter Server. When you add a host to vCenter Server, the agent is installed on the physical ESX/ESXi host. When you upgrade to vCenter Server 5.x, the agent residing on each ESX/ESXi host must be upgraded as well.

During a vCenter Server upgrade, the existing agent software is uninstalled and the updated agent software is installed in its place. If the upgrade fails, the updated agent software might not be installed and the host might become unreachable by vCenter Server 4.x or 5.x. To avoid this condition, you can run the vCenter Host Agent Pre-Upgrade Checker before you try to upgrade to vCenter Server 5.x.

The vCenter Host Agent Pre-Upgrade Checker checks to make sure that the agent software is ready to be upgraded. Some of the checks include checking to make sure that the host is reachable, the disk space is sufficient, the network is functioning, the file system is intact, and required patches are applied. Each time you run the tool, the system queries VMware.com and downloads any new updates for the tool. This action ensures that as new upgrade issues are discovered, the tool remains as useful as possible.

IMPORTANT A successful vCenter Host Agent pre-upgrade check does not guarantee a successful upgrade to vCenter Server 5.x. An upgrade to vCenter Server involves multiple components, and the tool checks only one component: the vCenter Host Agent. Also, the tool checks only known issues. Other issues might be present that the tool does not check.

The vCenter Host Agent Pre-Upgrade Checker does not fix the reported issues. You must resolve the reported issues manually and rerun the tool to verify that the issues are resolved.

For the procedure to run the vCenter Host Agent Pre-Upgrade Checker, see "Run the vCenter Host Agent Pre-Upgrade Checker," on page 57.

Run the vCenter Host Agent Pre-Upgrade Checker

The vCenter Host Agent Pre-Upgrade Checker reports known issues that might prevent a successful upgrade of the vCenter Host Agent software.

For more information about the vCenter Host Agent Pre-Upgrade Checker, see "About the vCenter Host Agent Pre-Upgrade Checker," on page 57.

Prerequisites

- Verify that the ESX/ESXi hosts are managed by vCenter Server.
- Verify that the vCenter Host Agent software is running on each managed ESX/ESXi host.
- Verify that you have Internet connectivity from the vCenter Server system. This allows new updates to be applied to the tool and allows you to view the reports and the Knowledge Base (KB) articles associated with the reports.
- Download the vCenter Server installer. See "Download the vCenter Server Installer," on page 59.

Procedure

1 In the software installer directory, double-click the `autorun.exe` file to start the installer.

2 Select **Host Agent Pre-Upgrade Checker** and click **Install**.

3 Select the DSN for the vCenter Server system you are upgrading from and select the login credentials that are appropriate for that DSN.

If you are not sure which credential type to select, check which authentication type is configured for the DSN (**Control Panel > Administrative Tools > ODBC Data Sources > System DSN**).

4 If the DSN requires a login for the credential type in use, enter a user name and password and click **Next**.

5 Select an option for scanning all hosts or specific hosts.

Option	Action
Scan all of the hosts	Select **Standard Mode** and click **Next**.
Specify hosts to scan	a Select **Custom Mode** and click **Next**. b Select the hosts to scan and click **Next**. To select all hosts in a cluster, double-click the cluster.

6 Click **Run Precheck**.

The tool takes 30-40 seconds for each host.

7 When the check is complete, click **Next**.

8 View the pre-upgrade reports.

- To view the report for an individual host, click the link next to the host name.
- To view a summary report for all hosts, click **View Report**.

You have a list of issues to resolve before you upgrade.

What to do next

From the report, use the linked KB articles to research and resolve the issues for each host. After you resolve the issues, rerun the vCenter Host Agent Pre-Upgrade Checker. Repeat this process until you resolve all the reported issues, and proceed with your upgrade.

Downtime During the vCenter Server Upgrade

When you upgrade vCenter Server, downtime is required for vCenter Server.

Expect downtime for vCenter Server as follows:

- The upgrade requires vCenter Server to be out of production for 40-50 minutes, depending on the size of the database. The database schema upgrade takes approximately 10-15 minutes of this time. This estimate does not include host reconnection after the upgrade.

  If Microsoft .NET Framework is not installed on the machine, a reboot is required before starting the vCenter Server installation.

- VMware Distributed Resource Scheduler does not work while the upgrade is in progress. VMware HA does work during the upgrade.

Downtime is not required for the ESX/ESXi hosts that vCenter Server is managing, or for virtual machines that are running on the hosts.

Download the vCenter Server Installer

Download the installer for vCenter Server, the vSphere Web Client, and associated vCenter components and support tools.

Prerequisites

Create a My VMware account at https://my.vmware.com/web/vmware/.

Procedure

1 Download the vCenter Server installer from the VMware Web site at https://my.vmware.com/web/vmware/downloads.

vCenter Server is part of VMware vSphere, listed under Datacenter & Cloud Infrastructure.

2 Confirm that the md5sum is correct.

See the VMware Web site topic Using MD5 Checksums at http://www.vmware.com/download/md5.html.

Microsoft SQL Database Set to Unsupported Compatibility Mode Causes vCenter Server Installation or Upgrade to Fail

vCenter Server installation with a Microsoft SQL database fails when the database is set to compatibility mode with an unsupported version.

Problem

The following error message appears: `The DB User entered does not have the required permissions needed to install and configure vCenter Server with the selected DB. Please correct the following error(s): %s`

Cause

The database version must be supported for vCenter Server. For SQL, even if the database is a supported version, if it is set to run in compatibility mode with an unsupported version, this error occurs. For example, if SQL 2008 is set to run in SQL 2000 compatibility mode, this error occurs.

Solution

- Make sure the vCenter Server database is a supported version and is not set to compatibility mode with an unsupported version. See the VMware Product Interoperability Matrixes at http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php?.

Upgrading vCenter Server 4

The vCenter Server upgrade includes a database schema upgrade and an upgrade of the vCenter Server software.

vSphere 5.1 introduced vCenter Single Sign-On as part of the vCenter Server management infrastructure. This change affects vCenter Server installation, upgrading, and operation. See "How vCenter Single Sign-On Affects vCenter Server Upgrades," on page 32.

This chapter includes the following topics:

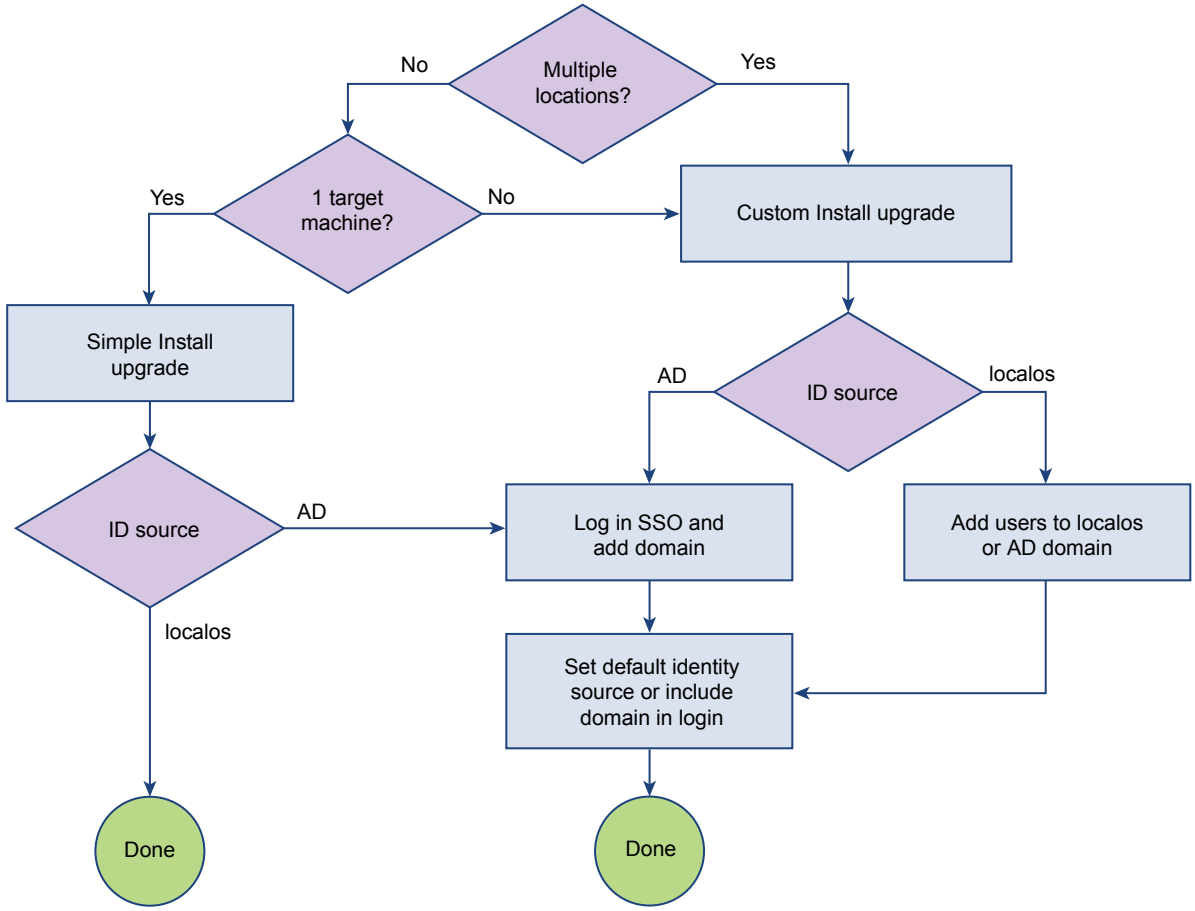
vCenter Server Upgrade and Sign-On Process for Environments that Do Not Include vCenter Single Sign-On

The upgrade process differs based on several factors. Understand the complete upgrade, vCenter Single Sign-On setup, and permission assignment process before you start. This topic explains how to perform the upgrade and user management if you upgrade from vSphere 5.0 or earlier, which does not include vCenter Single Sign-On.

If you are upgrading from vSphere 5.0 or earlier, your original environment does not include a vCenter Single Sign-On server. How you perform the upgrade, and whether you are required to add identity sources or assign permissions depends on your current environment and on what you intend to do, as shown in the following illustration.

NOTE This topic focuses on the most frequently encountered upgrade cases. It does not include a discussion of upgrading an installation that includes a vCenter Single Sign-On high availability deployment. See "Use Custom Install to Upgrade vCenter Server from a Version 5.1.x High Availability vCenter Single Sign-On Deployment," on page 84..

Figure 4-1. Upgrade and Sign In Process for Environments that Do Not Include vCenter Single Sign-On



The interaction proceeds as follows.

1 If your current environment is installed on different machines and potentially in different locations, it is easiest to have the target environment use the same layout.

   - If your current environment is distributed over several machines or several location, you can perform a Custom Install upgrade. (see step 4)

- If your current environment is not distributed over several machines or several locations, you can distribute the upgrade over multiple machines with a custom install (step 4) or continue placing all vCenter components on the same machine (step 2).

2 If all vCenter Server components are on the same host machine, you can upgrade with Simple Install. See "Use Simple Install to Upgrade vCenter Server and Required Components," on page 65. After you upgrade with the Simple Install process, local operating system users and the user administrator@vsphere.local can authenticate.

- If your environment was using only local operating system users, the localos identity source is sufficient. You can log in to vCenter Server as administrator@vsphere.local or any local operating system user who previously had permissions.
- If your environment was using Active Directory to manage users and permissions, go to Step 3.

3 If your pre-upgrade environment used Active Directory to manage users and permissions, the Active Directory domain is added to vCenter Single Sign-On as an identity source. Users who previously had permissions to access vCenter Server objects continue to have those permissions.

Only one default identity source is supported with vSphere 5.5, and the Active Directory identity source is initially not the default identity source. Users can log in only if they include the domain as part of the login (DOMAIN\user).

You can log in to the vCenter Single Sign-On server as administrator@vsphere.local and make the Active Directory domain the default identity source.

a Log in to the vCenter Single Sign-On server as administrator@vsphere.local and add the Active Directory domain as an identity source. See "Add a vCenter Single Sign-On Identity Source," on page 104.

b Make the Active Directory domain the default identity source. Only one default identity source is supported. Users from other domains can include the domain as part of the login (DOMAIN\user).

c Users who previously had permissions to access vCenter Server objects continue to have those permissions.

4 If you decide to install vCenter Server services on different machines, you can use a Custom Install upgrade process. See "Use Custom Install to Upgrade Version 5.0.x and Earlier vCenter Server and Required Components," on page 69.

a If your current environment supports only local operating system users, you must either make sure those users are available as localos users on the machine where vCenter Single Sign-On is installed, or you can add an Active Directory or OpenLDAP domain that includes those users.

b If your current environment supports an Active Directory domain, you can log in to the vCenter Single Sign-On server as administrator@vsphere.local and add the Active Directory domain to vCenter Single Sign-On. See "Add a vCenter Single Sign-On Identity Source," on page 104.

c You can either set the default identity source or users who log in to vCenter Server can include the domain name when they log in.

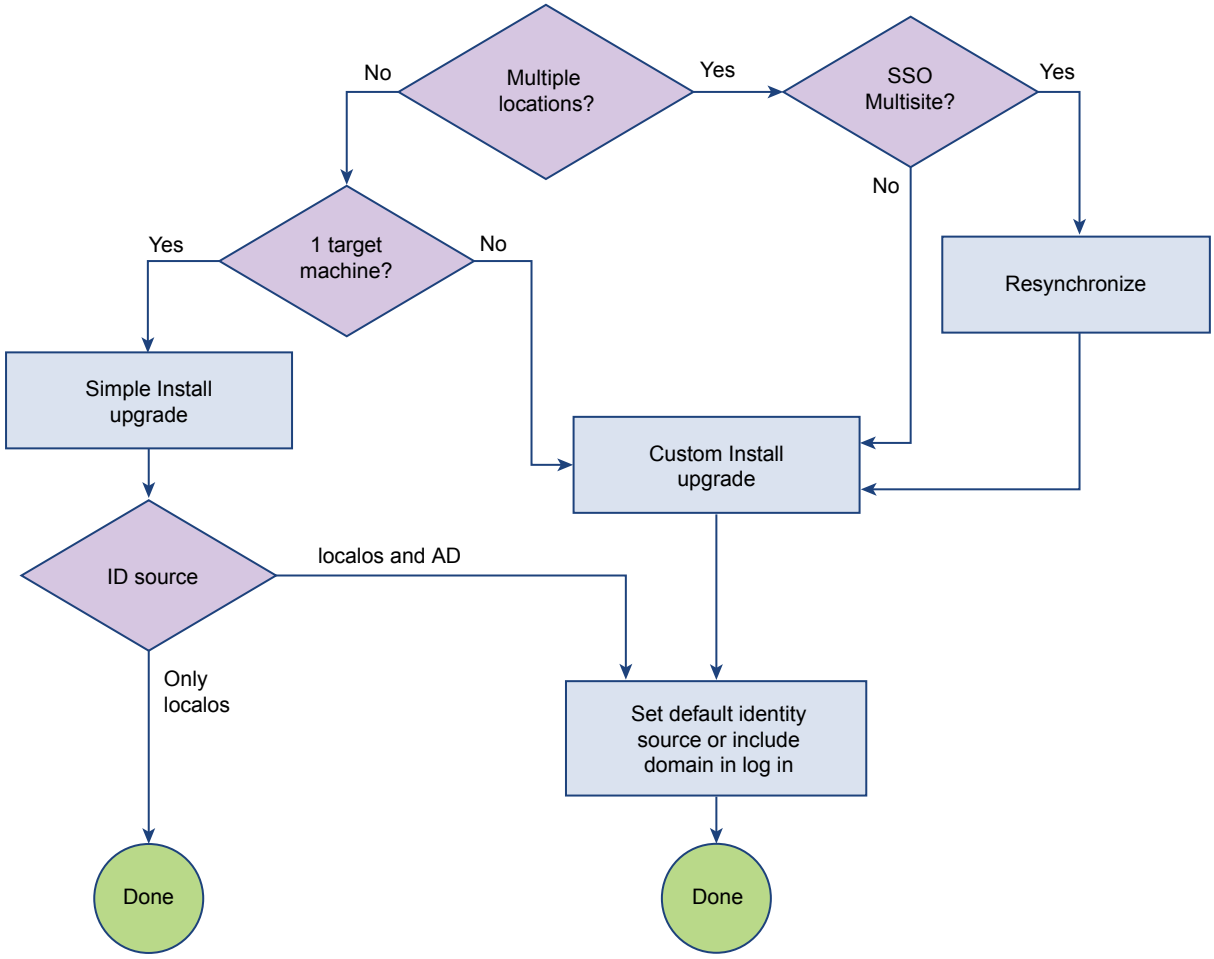
vCenter Server Upgrade and Sign-On Process for Environments with vCenter Single Sign-On

The upgrade process differs based on several factors. Understand the complete upgrade, vCenter Single Sign-On setup, and permission assignment process before you start. This topic explains how to perform the upgrade and user management if you upgrade from vSphere 5.1.x, which includes an earlier version of vCenter Single Sign-On.

If you are upgrading from vSphere 5.1.x, your original environment includes a vCenter Single Sign-On server. How you perform the upgrade, and whether you are required to add identity sources or assign permissions, depends on your current environment and on what you intend to do, as shown in the following illustration.

NOTE This topic focuses on the most frequently encountered upgrade cases. It does not include a discussion of upgrading an installation that includes a vCenter Single Sign-On high availability deployment. See "Use Custom Install to Upgrade vCenter Server from a Version 5.1.x High Availability vCenter Single Sign-On Deployment," on page 84.

Figure 4-2. Flowchart of vCenter Upgrade from Environments that Include vCenter Single Sign-On



The interaction proceeds as follows.

1 If your current environment is installed on different machines and potentially in different locations, it is easiest to have the target environment use a similar layout.

With vSphere 5.5, multiple vCenter Server systems can use a single vCenter Single Sign-On system.

- If your current environment uses vCenter Single Sign-On multisite, resynchronize your environment. See Knowledge Base articles http://kb.vmware.com/kb/2042849 and http://kb.vmware.com/kb/2038677, and start a Custom Install upgrade. See "Use Custom Install to Upgrade Version 5.0.x and Earlier vCenter Server and Required Components," on page 69. Which users can access vCenter Single Sign-On and vCenter Server depends on the identity sources that are defined before the upgrade. See step 3.
- If your current environment does not use vCenter Single Sign-On multisite, you can distribute the upgrade over multiple machines with a Custom Install or continue placing all vCenter services on the same machine (step 2).

2 If all vCenter Server components are on the same host machine, you can upgrade with Simple Install. See "Use Simple Install to Upgrade vCenter Server and Required Components," on page 65. After you upgrade with the Simple Install process, local operating system users and the user administrator@vsphere.local can authenticate.

- If your environment was using only local operating system users, the localos identity source is sufficient. You can log in to vCenter Server as administrator@vsphere.local, or as any local operating system user who previously had permissions.

  NOTE Local operating users in embedded groups are no longer available. You can add those groups explicitly.

- If your environment was using an Active Directory or OpenLDAP identity source, those identity sources are included with vCenter Single Sign-On after the upgrade, but they are not the default identity source. Go to Step 3.

3 If your environment was using an Active Directory or OpenLDAP identity source.

- Users in the default identity source (localos by default) can log in to vCenter Server if they had permission to do so previously.
- Users in other identity sources can log in to vCenter Server if they use the domain name and password, for example, DOMAIN1\user1.
- You can log in to vCenter Single Sign-On as administrator@vsphere.local to make the Active Directory or OpenLDAP identity source the default identity source.

Use Simple Install to Upgrade vCenter Server and Required Components

vCenter Server versions 5.1 and later require the vCenter Single Sign-On and vCenter Inventory Service components. Depending on your existing vCenter Server installation, you can use the Simple Install option to upgrade to vCenter Server, including vCenter Single Sign-On, the vSphere Web Client, and Inventory Service, all on a single host machine.

You can use Simple Install to upgrade vCenter Server if you have a version 4.x, 5.0.x, or 5.1.x vCenter Server installation that is supported for upgrade, and all vCenter Server components in the installation you are upgrading are on the same host machine. See the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php. Depending on the version you are upgrading from, the Simple Install option installs or upgrades Single Sign-On, and upgrades the vSphere Web Client, Inventory Service, and vCenter Server.

Alternatively, you can upgrade vCenter Server components separately, for installations in which the location and configuration of the components is customized. See "Use Custom Install to Upgrade a Basic vCenter Single Sign-On Deployment of Version 5.1.x vCenter Server and Required Components," on page 78, "Use Custom Install to Upgrade vCenter Server from a Version 5.1.x High Availability vCenter Single Sign-On Deployment," on page 84, or "Use Custom Install to Upgrade vCenter Server from a Version 5.1.x Multisite vCenter Single Sign-On Deployment," on page 93.

NOTE You cannot use Simple Install to upgrade from vCenter Server 5.5 to a later 5.5.x version, for example, from version 5.5.0 to 5.5 Update 1. If you attempt to do so, the installer displays the message `vCenter Package components already installed. Please install any remaining components by clicking on the respective links one the left.` This means, that some of the vCenter Server components of the 5.5.x version might be already installed and you must upgrade all of the other components by using the individual installers. To upgrade from vCenter Server 5.5 to a later 5.5.x version, you must use the individual vCenter Single Sign-On, vSphere Web Client, vCenter Inventory Service, and vCenter Server installers. See "Use Custom Install to Upgrade a Basic vCenter Single Sign-On Deployment of Version 5.1.x vCenter Server and Required Components," on page 78.

Prerequisites

See "Prerequisites for the vCenter Server Upgrade," on page 48.

Procedure

1 Install or Upgrade vCenter Single Sign-On and the vSphere Web Client as Part of a vCenter Server Simple Install on page 66

   Create or upgrade the only node in a basic, Simple Install vCenter Single Sign-On installation, and install or upgrade the vSphere Web Client and vCenter Inventory Service.

2 Upgrade vCenter Inventory Service as Part of vCenter Server Simple Install on page 68

   You can Install or upgrade vCenter Single Sign-On, the vSphere Web Client, vCenter Inventory Service, and vCenter Server together on a single host machine using the vCenter Server Simple Install option.

3 Upgrade vCenter Server as Part of a Simple Install on page 68

   You can upgrade vCenter Server as part of a Simple Install after you install vCenter Single Sign-On, upgrade the vSphere Web Client, and upgrade Inventory Service.

Install or Upgrade vCenter Single Sign-On and the vSphere Web Client as Part of a vCenter Server Simple Install

Create or upgrade the only node in a basic, Simple Install vCenter Single Sign-On installation, and install or upgrade the vSphere Web Client and vCenter Inventory Service.

If you are upgrading a vCenter Server deployment that includes vCenter Single Sign-On, this procedure upgrades the existing vCenter Single Sign-On instance, and does not include all the steps listed below for a new installation.

You can use Simple Install for the first vCenter Single Sign-On and vCenter Server in a deployment with multiple vCenter Servers. Succeeding instances of vCenter Single Sign-On and vCenter Server in the same deployment must be installed by using Custom Install. For more information about vCenter Single Sign-On, see "How vCenter Single Sign-On Affects vCenter Server Upgrades," on page 32 and the *vSphere Security* documentation.

NOTE vCenter Server 5.5 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPv4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

Prerequisites

- See "Prerequisites for the vCenter Server Upgrade," on page 48.
- Download the vCenter Server installer. See "Download the vCenter Server Installer," on page 59.

Procedure

1. In the software installer directory, double-click the `autorun.exe` file to start the installer.
2. Select **vCenter™ Simple Install**, and click **Install**.
3. Follow the prompts in the installation wizard to choose the installer language, and agree to the end user patent and license agreements.
4. If the prerequisites check screen shows any problems, cancel the installation, correct the problems, and restart the installer.
5. Set the password for the vCenter Single Sign-On administrator account.

   This is the password for the user administrator@vsphere.local. vsphere.local is a new domain that is created by vCenter Single Sign-On. After installation, you can log in to vCenter Single Sign-On and in to vCenter Server as adminstrator@vsphere.local.

   By default, the password must have at least eight characters, at least one lowercase character, one uppercase character, one number, and one special character. See the *vSphere Security* documentation for information about changing the password policy. The following characters are not supported in passwords: non-ASCII characters, semicolon (;), double quotation mark ("), single quotation mark ('), circumflex (^), and backslash (\).
6. Enter the site name for vCenter Single Sign-On.

   The site name becomes important if you are using vCenter Single Sign-On in multiple locations. Choose your own name for the vCenter Single Sign-On site.

   NOTE You cannot change the site name at a later time.
7. Accept or change the HTTPS port for vCenter Single Sign-On.
8. Select the folder in which to install vCenter Single Sign-On.

   The installation path cannot contain any of the following characters: non-ASCII characters, commas (,), periods (.), exclamation points (!), pound signs (#), at signs (@), or percentage signs (%).
9. Review the installation options and click **Install.**

The vCenter Single Sign-On installation or upgrade begins. When the vCenter Single Sign-On installation or upgrade is complete, the installer proceeds with the vSphere Web Client and vCenter Inventory Service installations or upgrades.

No input is required for a Simple Install upgrade of the vSphere Web Client.

NOTE After each component is installed or upgraded, the installer might take a few minutes to start the installer for the next component.

Upgrade vCenter Inventory Service as Part of vCenter Server Simple Install

You can Install or upgrade vCenter Single Sign-On, the vSphere Web Client, vCenter Inventory Service, and vCenter Server together on a single host machine using the vCenter Server Simple Install option.

Procedure

1 Choose whether to keep the existing database or replace it with a new empty database.

2 Click **Install**.

Inventory Service is upgraded, and the vCenter Server upgrade wizard starts.

What to do next

Upgrade vCenter Server. Proceed to "Upgrade vCenter Server as Part of a Simple Install," on page 68.

Upgrade vCenter Server as Part of a Simple Install

You can upgrade vCenter Server as part of a Simple Install after you install vCenter Single Sign-On, upgrade the vSphere Web Client, and upgrade Inventory Service.

This procedure continues the vCenter Server upgrade using Simple Install from the subtask "Upgrade vCenter Inventory Service as Part of vCenter Server Simple Install," on page 68. If the upgrade fails, no automatic rollback occurs to the previous vCenter Server version.

NOTE vCenter Server 5.5 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPv4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

Prerequisites

- See "Prerequisites for the vCenter Server Upgrade," on page 48.

Procedure

1 (Optional) Enter your license key.

IMPORTANT If you do not enter a license key, your license will expire. After the installation, you can connect to the vCenter Server and reenter the license key.

2 Enter or confirm your database credentials.

3 Select whether to upgrade the vCenter Server database.

- Select **Upgrade existing vCenter Server database** to continue with the upgrade to vCenter Server.
- Select **Do not upgrade existing vCenter Server database** if you do not have a backup copy of your database.

  You cannot continue the upgrade.

4 Click **I have taken a backup of the existing vCenter Server database and SSL certificates**.

5 Select how to upgrade vCenter Agent.

Option	Description
Automatic	To automatically upgrade vCenter Agent on all the hosts in the vCenter Server inventory.
Manual	If one of the following applies: ■ You need to control the timing of vCenter Agent upgrades on specific hosts. ■ vCenter Agent is installed on each host in the inventory to enable vCenter Server to manage the host. vCenter Agent must be upgraded when vCenter Server is upgraded.

vCenter Agent is installed on each host in the inventory to enable vCenter Server to manage the host. vCenter Agent must be upgraded when vCenter Server is upgraded.

6 Select the account for the vCenter Service to run in.

Option	Description
SYSTEM Account	Select the **Use Windows Local System Account** check box, type the fully qualified domain name of the vCenter Server host, and click **Next**. You cannot use the Use Windows Local System Account account if you are using the bundled database or SQL Server with Windows authentication.
User-specified account	Deselect the **Use Windows Local System Account** check box, type the account password and the fully qualified domain name of the vCenter Server host, and click **Next**.

7 Accept or change the port numbers to connect to vCenter Server.

8 (Optional) Select **Increase the number of available ephemeral ports**.

9 Select the size of your vCenter Server inventory to allocate memory for several Java services that are used by vCenter Server.

This setting determines the maximum JVM heap settings for VMware VirtualCenter Management Webservices (Tomcat), Inventory Service, and Profile-Driven Storage Service. You can adjust this setting after installation if the number of hosts in your environment changes. See the recommendations in the topic vCenter Server Hardware Requirements.

10 Click **Install**.

The vCenter Simple Install is complete.

Use Custom Install to Upgrade Version 5.0.x and Earlier vCenter Server and Required Components

You can upgrade vCenter Server and other vCenter components separately to customize the location and configuration of each component.

This procedure upgrades vCenter Server versions 5.0.x and earlier, which do not include vCenter Single Sign-On. If you are upgrading vCenter Server 5.1.x, see one of the following procedures:

- "Use Custom Install to Upgrade a Basic vCenter Single Sign-On Deployment of Version 5.1.x vCenter Server and Required Components," on page 78.
- "Use Custom Install to Upgrade vCenter Server from a Version 5.1.x High Availability vCenter Single Sign-On Deployment," on page 84.
- "Use Custom Install to Upgrade vCenter Server from a Version 5.1.x Multisite vCenter Single Sign-On Deployment," on page 93.

For most basic vCenter Single Sign-On deployments, if all components are on the same host machine, you can upgrade vCenter Single Sign-On, the vSphere Web Client, Inventory Service, and vCenter Server together on a single host machine using the vCenter Server Simple Install option.

See "Use Simple Install to Upgrade vCenter Server and Required Components," on page 65.

NOTE vCenter Server 5.5 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPv4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

Prerequisites

- Review Chapter 3, "Preparing for the Upgrade to vCenter Server," on page 31.
- See "Prerequisites for the vCenter Server Upgrade," on page 48

Procedure

1 Install the First or Only vCenter Single Sign-On Instance in a vCenter Server Deployment on page 70

Create the only vCenter Single Sign-On instance in a basic vCenter Single Sign-On installation or the first vCenter Single Sign-On instance in a deployment with multiple vCenter Single Sign-On instances.

2 (Optional) Install an Additional vCenter Single Sign-On Node at an Existing Site on page 72

Create an additional vCenter Single Sign-On node at an existing vCenter Single Sign-On installation. An additional vCenter Single Sign-On node might be useful if your deployment includes multiple vCenter Server instances.

3 (Optional) Install an Additional vCenter Single Sign-On Node at a New Site on page 73

Create an additional vCenter Single Sign-On node for a multisite vCenter Single Sign-On installation. An additional node can be useful if you need multiple vCenter Server instances in different locations. Authentication information is replicated between vCenter single Sign-On instances that are related.

4 Install or Upgrade the vSphere Web Client on page 74

The vSphere Web Client lets you connect to a vCenter Server system to manage your vSphere deployment through a browser.

5 Upgrade vCenter Inventory Service Separately by Using Custom Install on page 75

You can use Custom Install to upgrade vCenter Single Sign-On, vCenter Inventory Service, and vCenter Server separately to customize the location and configuration of the components.

6 Upgrade vCenter Server Separately by Using Custom Install on page 76

You can upgrade vCenter Server separately after installing vCenter Single Sign-On, and upgrading Inventory Service.

Install the First or Only vCenter Single Sign-On Instance in a vCenter Server Deployment

Create the only vCenter Single Sign-On instance in a basic vCenter Single Sign-On installation or the first vCenter Single Sign-On instance in a deployment with multiple vCenter Single Sign-On instances.

These instructions let you install or upgrade vCenter Single Sign-On only. You must install or upgrade vCenter Single Sign-On and upgrade Inventory Service before upgrading vCenter Server. For most deployments, you can install vCenter Single Sign-On, the vSphere Web Client, vCenter Inventory Service, and vCenter Server together on a single host machine by using vCenter Server Simple Install. See "vCenter Single Sign-On Deployment Modes," on page 33 and "Use Simple Install to Upgrade vCenter Server and Required Components," on page 65.

For more information about vCenter Single Sign-On, see "How vCenter Single Sign-On Affects vCenter Server Upgrades," on page 32and the *vSphere Security* documentation.

NOTE vCenter Server 5.5 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPv4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

Prerequisites

- Review "vCenter Single Sign-On Deployment Modes," on page 33.
- Review "How vCenter Single Sign-On Affects vCenter Server Upgrades," on page 32.
- See "Prerequisites for the vCenter Server Upgrade," on page 48
- Download the vCenter Server installer. See "Download the vCenter Server Installer," on page 59.

Procedure

1. In the software installer directory, double-click the `autorun.exe` file to start the installer.
2. Select **vCenter Single Sign-On** and click **Install**.
3. Follow the prompts in the installation wizard to choose the installer language, and agree to the end user patent and license agreements.
4. If the prerequisites check screen shows any problems, cancel the installation, correct the problems, and restart the installer.
5. Set the password for the vCenter Single Sign-On administrator account.

   This is the password for the user administrator@vsphere.local. vsphere.local is a new domain that is created by vCenter Single Sign-On. After installation, you can log in to vCenter Single Sign-On and in to vCenter Server as adminstrator@vsphere.local.

   By default, the password must have at least eight characters, at least one lowercase character, one uppercase character, one number, and one special character. See the *vSphere Security* documentation for information about changing the password policy. The following characters are not supported in passwords: non-ASCII characters, semicolon (;), double quotation mark ("), single quotation mark ('), circumflex (^), and backslash (\).
6. Accept or change the HTTPS port for vCenter Single Sign-On.
7. Select the deployment mode **vCenter Single Sign-On for your first vCenter Server**.
8. Enter the site name for vCenter Single Sign-On.

   The site name becomes important if you are using vCenter Single Sign-On in multiple locations. Choose your own name for the vCenter Single Sign-On site.

   NOTE You cannot change the site name at a later time.
9. Review the installation options and click **Install.**

vCenter Single Sign-On is installed.

After vCenter Single Sign-On is installed or upgraded, the following default identity sources and users are available:

localos	All local operating system users. These users can be granted permissions to vCenter Server. If you are upgrading, those users who already have permissions keep those permissions.
vsphere.local	Contains all users who have administrator access to the vCenter Single Sign-On server. Initially, only the user administrator is defined.

What to do next

To deploy vCenter Server with multiple vCenter Single Sign-On instances, install an additional vCenter Single Sign-On at an existing or new site. See "(Optional) Install an Additional vCenter Single Sign-On Node at an Existing Site," on page 72 or "(Optional) Install an Additional vCenter Single Sign-On Node at a New Site," on page 73. If your vCenter Server deployment requires only one vCenter Single-Sign-On instance, install the vSphere Web Client. See "Install or Upgrade the vSphere Web Client," on page 128.

To add other identity sources, such as a native Active Directory (Integrated Windows Authentication) domain or an OpenLDAP directory service, see "Add a vCenter Single Sign-On Identity Source," on page 104.

(Optional) Install an Additional vCenter Single Sign-On Node at an Existing Site

Create an additional vCenter Single Sign-On node at an existing vCenter Single Sign-On installation. An additional vCenter Single Sign-On node might be useful if your deployment includes multiple vCenter Server instances.

Prerequisites

- Review "vCenter Single Sign-On Deployment Modes," on page 33.
- See "Prerequisites for the vCenter Server Upgrade," on page 48.
- Install the first node in the vCenter Single Sign-On installation. See "Install the First or Only vCenter Single Sign-On Instance in a vCenter Server Deployment," on page 70.

Procedure

1. In the software installer directory, double-click the `autorun.exe` file to start the installer.
2. Select **vCenter Single Sign-On** and click **Install**.
3. Follow the prompts in the installation wizard to choose the installer language, and agree to the end user patent and license agreements.
4. Accept or change the HTTPS port for vCenter Single Sign-On.
5. Select the deployment mode **vCenter Single Sign-On for an additional vCenter Server in an existing site**.
6. Enter the information to point this additional node to the first vCenter Single Sign-On server.

   NOTE If the primary node is in a high-availability cluster, enter the address of the primary node load balancer.

   a. Enter the **Partner host name**.

      The partner host name is the DNS name of the existing vCenter Single Sign-On server to replicate from.

   b. Enter the password for the vCenter Single Sign-On administrator account of the existing vCenter Single Sign-On server (administrator@vsphere.local).

7 Select an existing site as the partner or enter a new site.

8 Click **Install**.

(Optional) Install an Additional vCenter Single Sign-On Node at a New Site

Create an additional vCenter Single Sign-On node for a multisite vCenter Single Sign-On installation. An additional node can be useful if you need multiple vCenter Server instances in different locations. Authentication information is replicated between vCenter single Sign-On instances that are related.

Prerequisites

- Review "vCenter Single Sign-On Deployment Modes," on page 33.
- See "Prerequisites for the vCenter Server Upgrade," on page 48.
- Install the first node in the vCenter Single Sign-On installation. See "Install the First or Only vCenter Single Sign-On Instance in a vCenter Server Deployment," on page 70.

Procedure

1 In the software installer directory, double-click the `autorun.exe` file to start the installer.

2 Select **vCenter Single Sign-On** and click **Install**.

3 Follow the prompts in the installation wizard to choose the installer language, and agree to the end user patent and license agreements.

4 Accept or change the HTTPS port for vCenter Single Sign-On.

5 Select the deployment mode **vCenter Single Sign-On for an additional vCenter Server with a new site**.

6 Enter the information to point this additional node to the first vCenter Single Sign-On server.

NOTE If the primary node is in a high-availability cluster, enter the address of the primary node load balancer.

   a Enter the **Partner host name**.

   The partner host name is the DNS name of the existing vCenter Single Sign-On server to replicate from.

   b Enter the password for the vCenter Single Sign-On administrator account of the existing vCenter Single Sign-On server (administrator@vsphere.local).

7 Select an existing site as the partner or enter a new site.

8 Click **Install.**

The additional vCenter Single Sign-On server is installed.

What to do next

Repeat this procedure for each additional node.

Install or Upgrade the vSphere Web Client

The vSphere Web Client lets you connect to a vCenter Server system to manage your vSphere deployment through a browser.

If an earlier version of the vSphere Web Client is installed, this procedure upgrades the vSphere Web Client.

NOTE vCenter Server 5.5 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPv4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

Prerequisites

- Download the vCenter Server installer. See "Download the vCenter Server Installer," on page 59.
- Verify that the system has an Internet connection.
- Verify that the system meets the software requirements for the vSphere Web Client. See "vSphere Web Client Software Requirements," on page 22.
- Before you install or upgrade any vSphere product, synchronize the clocks of all machines on the vSphere network. See "Synchronizing Clocks on the vSphere Network," on page 53.
- Install vCenter Single Sign-On, or upgrade to the current version.
- Verify that the vSphere Web Client and vCenter Server are registered to the same vCenter Single Sign-On server, to ensure that the vSphere Web Client can access the vCenter Server inventory.
- Close all browsers before installing or uninstalling the vSphere Web Client.
- Log in as a member of the Administrators group on the host machine, with a user name that does not contain any non-ASCII characters.

Procedure

1. In the software installer directory, double-click the `autorun.exe` file to start the installer.
2. Select **vSphere Web Client** and click **Install**.
3. Follow the prompts in the installation wizard to choose the installer language, and agree to the end user patent and license agreements.
4. Either accept the default destination folder or click **Change** to select another location.

   The installation path cannot contain any of the following characters: non-ASCII characters, commas (,), periods (.), exclamation points (!), pound signs (#), at signs (@), or percentage signs (%).

   If 8.3 name creation is disabled on the host machine, do not install the vSphere Web Clientin a directory that does not have an 8.3 short name or has a name that contains spaces. This situation will make the vSphere Web Client inaccessible.
5. Accept or change the default port settings.
6. Enter the information to register the vSphere Web Client with vCenter Single Sign-On.

   The vCenter Single Sign-On administrator user name is administrator@vsphere.local, and the password must match the password you entered for the administrator user when you installed vCenter Single Sign-On. The Lookup Service URL takes the form https://*SSO_host_FQDN_or_IP*:7444/lookupservice/sdk, where 7444 is the default vCenter Single Sign-On HTTPS port number. Your entry should match the entry you made when you installed vCenter Single Sign-On. If you entered a different port number when you installed vCenter Single Sign-On, use that port number.

7 Click **Install**.

8 Start the vSphere Web Client by taking one of the following actions.

- If you are starting the vSphere Web Client for the first time, open a supported browser, and go to https://*vSphere_Web_Client_host_name_or_IP*:9443/vsphere-client.
- In subsequent sessions, you can start the vSphere Web Client from the Windows Start menu, by selecting **Programs > VMware > VMware vSphere Web Client > vSphere Web Client**.

NOTE After you upgrade the vSphere Web Client, when you log in for the first time, you may see the error message `Failed to navigate to desired location`. This can happen when a vSphere Web Client session from the previous version remains open when you upgrade. In this case, refresh the browser and log in again.

Upgrade vCenter Inventory Service Separately by Using Custom Install

You can use Custom Install to upgrade vCenter Single Sign-On, vCenter Inventory Service, and vCenter Server separately to customize the location and configuration of the components.

These instructions upgrade vCenter Inventory Service only. You must install or upgrade vCenter Single Sign-On before upgrading Inventory Service and vCenter Server.

NOTE vCenter Server 5.5 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPv4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

Prerequisites

- Review "vCenter Single Sign-On Deployment Modes," on page 33.
- Review "How vCenter Single Sign-On Affects vCenter Server Upgrades," on page 32.
- See "Prerequisites for the vCenter Server Upgrade," on page 48
- Download the vCenter Server Installer.
- Upgrade vCenter Single Sign-On.

Procedure

1 In the software installer directory, double-click the `autorun.exe` file to start the installer.

2 Select **vCenter Inventory Service** and click **Install.**

3 Follow the prompts in the installation wizard to choose the installer language, and agree to the end user patent and license agreements.

4 If you are upgrading or reinstalling an existing instance of Inventory Service, choose whether to keep the existing database or replace it with a new empty database.

5 Click **Install**.

Inventory Service is upgraded.

Upgrade vCenter Server Separately by Using Custom Install

You can upgrade vCenter Server separately after installing vCenter Single Sign-On, and upgrading Inventory Service.

Alternatively, you can upgrade vCenter Server as part of a Simple Install. See "Use Simple Install to Upgrade vCenter Server and Required Components," on page 65 and "How vCenter Single Sign-On Affects vCenter Server Upgrades," on page 32.

This procedure requires downtime for the vCenter Server that you are upgrading. You do not need to turn off virtual machines.

If an earlier version of vCenter Server is on your machine, the vCenter Server installer detects and upgrades it. If the upgrade fails, no automatic rollback occurs to the previous vCenter Server version.

NOTE vCenter Server 5.5 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPv4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

Prerequisites

- Review "vCenter Single Sign-On Deployment Modes," on page 33.
- Review "How vCenter Single Sign-On Affects vCenter Server Upgrades," on page 32.
- See "Prerequisites for the vCenter Server Upgrade," on page 48
- Install vCenter Single Sign-On and Inventory Service.

Procedure

1. In the software installer directory, double-click the `autorun.exe` file to start the installer.
2. Select **vCenter Server** and click **Install**.
3. Follow the prompts in the installation wizard to choose the installer language, and agree to the end user patent and license agreements.
4. Enter or confirm your database credentials.
5. Select whether to upgrade the vCenter Server database.
   - Select **Upgrade existing vCenter Server database** to continue with the upgrade to vCenter Server.
   - Select **Do not upgrade existing vCenter Server database** if you do not have a backup copy of your database.

     You cannot continue the upgrade.
6. Click **I have taken a backup of the existing vCenter Server database and SSL certificates**.

7 Select how to upgrade vCenter Agent.

Option	Description
Automatic	To automatically upgrade vCenter Agent on all the hosts in the vCenter Server inventory.
Manual	If one of the following applies: ■ You need to control the timing of vCenter Agent upgrades on specific hosts. ■ vCenter Agent is installed on each host in the inventory to enable vCenter Server to manage the host. vCenter Agent must be upgraded when vCenter Server is upgraded.

vCenter Agent is installed on each host in the inventory to enable vCenter Server to manage the host. vCenter Agent must be upgraded when vCenter Server is upgraded.

8 Select the account for the vCenter Service to run in.

Option	Description
SYSTEM Account	Select the **Use Windows Local System Account** check box, type the fully qualified domain name of the vCenter Server host, and click **Next**. You cannot use the Use Windows Local System Account account if you are using the bundled database or SQL Server with Windows authentication.
User-specified account	Deselect the **Use Windows Local System Account** check box, type the account password and the fully qualified domain name of the vCenter Server host, and click **Next**.

9 Accept or change the port numbers to connect to vCenter Server.

10 (Optional) Select **Increase the number of available ephemeral ports**.

11 Select the size of your vCenter Server inventory to allocate memory for several Java services that are used by vCenter Server.

This setting determines the maximum JVM heap settings for VMware VirtualCenter Management Webservices (Tomcat), Inventory Service, and Profile-Driven Storage Service. You can adjust this setting after installation if the number of hosts in your environment changes. See the recommendations in the topic vCenter Server Hardware Requirements.

12 Enter the information to register vCenter Server with vCenter Single Sign-On.

The vCenter Single Sign-On administrator user name is administrator@vsphere.local, and the password must match the password you entered when you installed vCenter Single Sign-On. The Lookup Service URL takes the form https://*SSO_host_FQDN_or_IP*:7444/lookupservice/sdk, where 7444 is the default vCenter Single Sign-On HTTPS port number. Your entry should match the entry you made when you installed vCenter Single Sign-On. If you entered a different port number when you installed vCenter Single Sign-On, use that port number.

NOTE If you installed vCenter Single Sign-On in a vCenter Server Appliance, you can enter the vCenter Single Sign-On administrator user as root@localos. In this case, the password is the root password of the vCenter Server Appliance. The Lookup Service URL takes the form https://*vCenter_Appliance_IP_or_host_name*:{7444}/lookupservice/sdk.

13 Enter the Inventory Service URL.

The Inventory Service URL takes the form https://*Inventory_Service_host_FQDN_or_IP*:10443. 10443 is the default Inventory Service HTTPS port number. If you entered a different port number when you installed Inventory Service, use that port number here.

14 Click **Install**.

Installation might take several minutes. Multiple progress bars appear during the installation of the selected components.

What to do next

Review the topics in Chapter 5, "After You Upgrade vCenter Server," on page 127 for other postupgrade actions you might want to take.

Use Custom Install to Upgrade a Basic vCenter Single Sign-On Deployment of Version 5.1.x vCenter Server and Required Components

You can upgrade vCenter and components separately to customize the location and configuration of the components. The basic vCenter Single Sign-On deployment contains only one vCenter Single Sign-On node.

For most basic vCenter Single Sign-On deployments, with all components on the same host machine, you can upgrade vCenter Single Sign-On, the vSphere Web Client, vCenter Inventory Service, and vCenter Server together on a single host machine using the vCenter Server Simple Install option.

See "Use Simple Install to Upgrade vCenter Server and Required Components," on page 65.

NOTE vCenter Server 5.5 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPv4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

Prerequisites

- Review the topics in Chapter 3, "Preparing for the Upgrade to vCenter Server," on page 31.
- See "Prerequisites for the vCenter Server Upgrade," on page 48

Procedure

1 Install or Upgrade vCenter Single Sign-On in a Basic Deployment on page 79

Create or upgrade vCenter Single Sign-On in a vCenter Single Sign-On installation.

2 Install or Upgrade the vSphere Web Client on page 80

The vSphere Web Client lets you connect to a vCenter Server system to manage your vSphere deployment through a browser.

3 Upgrade vCenter Inventory Service Separately by Using Custom Install on page 81

You can use Custom Install to upgrade vCenter Single Sign-On, vCenter Inventory Service, and vCenter Server separately to customize the location and configuration of the components.

4 Upgrade vCenter Server Separately by Using Custom Install on page 82

You can upgrade vCenter Server separately after installing vCenter Single Sign-On, and upgrading Inventory Service.

Install or Upgrade vCenter Single Sign-On in a Basic Deployment

Create or upgrade vCenter Single Sign-On in a vCenter Single Sign-On installation.

These instructions let you install or upgrade vCenter Single Sign-On only. You must install or upgrade vCenter Single Sign-On and upgrade Inventory Service before upgrading vCenter Server. For most deployments, you can install vCenter Single Sign-On, the vSphere Web Client, vCenter Inventory Service, and vCenter Server together on a single host machine by using vCenter Server Simple Install. See "vCenter Single Sign-On Deployment Modes," on page 33 and "Use Simple Install to Upgrade vCenter Server and Required Components," on page 65.

For more information about vCenter Single Sign-On, see "How vCenter Single Sign-On Affects vCenter Server Upgrades," on page 32 and the *vSphere Security* documentation.

NOTE vCenter Server 5.5 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPv4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

Prerequisites

- Review "vCenter Single Sign-On Deployment Modes," on page 33.
- Review "How vCenter Single Sign-On Affects vCenter Server Upgrades," on page 32.
- See "Prerequisites for the vCenter Server Upgrade," on page 48
- Download the vCenter Server installer. See "Download the vCenter Server Installer," on page 59.

Procedure

1. In the software installer directory, double-click the `autorun.exe` file to start the installer.
2. Select **vCenter Single Sign-On** and click **Install**.
3. Follow the prompts in the installation wizard to choose the installer language, and agree to the end user patent and license agreements.
4. If the prerequisites check screen shows any problems, cancel the installation, correct the problems, and restart the installer.
5. If you are installing a new instance of vCenter Single Sign-On, proceed to Step 6Step 7. If you are upgrading an existing installation of vCenter Single Sign-On, take the following steps:
   a. Enter the password for the vCenter Single Sign-On administrator account.
   b. Proceed to Step 10.
6. Set the password for the vCenter Single Sign-On administrator account.

   This is the password for the user administrator@vsphere.local. vsphere.local is a new domain that is created by vCenter Single Sign-On. After installation, you can log in to vCenter Single Sign-On and in to vCenter Server as adminstrator@vsphere.local.

   By default, the password must have at least eight characters, at least one lowercase character, one uppercase character, one number, and one special character. See the *vSphere Security* documentation for information about changing the password policy. The following characters are not supported in passwords: non-ASCII characters, semicolon (;), double quotation mark ("), single quotation mark ('), circumflex (^), and backslash (\).
7. Accept or change the HTTPS port for vCenter Single Sign-On.
8. Select the deployment mode **vCenter Single Sign-On for your first vCenter Server**.

9 Enter the site name for vCenter Single Sign-On.

The site name becomes important if you are using vCenter Single Sign-On in multiple locations. Choose your own name for the vCenter Single Sign-On site.

NOTE You cannot change the site name at a later time.

10 Review the installation options and click **Install**.

vCenter Single Sign-On is installed or upgraded.

After vCenter Single Sign-On is installed or upgraded, the following default identity sources and users are available:

localos	All local operating system users. These users can be granted permissions to vCenter Server. If you are upgrading, those users who already have permissions keep those permissions.
vsphere.local	Contains all users who have administrator access to the vCenter Single Sign-On server. Initially, only the user administrator is defined.

To add other identity sources, such as a native Active Directory (Integrated Windows Authentication) domain or an OpenLDAP directory service, see "Add a vCenter Single Sign-On Identity Source," on page 104.

What to do next

Upgrade the vSphere Web Client. See "Install or Upgrade the vSphere Web Client," on page 128.

Install or Upgrade the vSphere Web Client

The vSphere Web Client lets you connect to a vCenter Server system to manage your vSphere deployment through a browser.

If an earlier version of the vSphere Web Client is installed, this procedure upgrades the vSphere Web Client.

NOTE vCenter Server 5.5 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPv4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

Prerequisites

- Download the vCenter Server installer. See "Download the vCenter Server Installer," on page 59.
- Verify that the system has an Internet connection.
- Verify that the system meets the software requirements for the vSphere Web Client. See "vSphere Web Client Software Requirements," on page 22.
- Before you install or upgrade any vSphere product, synchronize the clocks of all machines on the vSphere network. See "Synchronizing Clocks on the vSphere Network," on page 53.
- Install vCenter Single Sign-On, or upgrade to the current version.
- Verify that the vSphere Web Client and vCenter Server are registered to the same vCenter Single Sign-On server, to ensure that the vSphere Web Client can access the vCenter Server inventory.
- Close all browsers before installing or uninstalling the vSphere Web Client.
- Log in as a member of the Administrators group on the host machine, with a user name that does not contain any non-ASCII characters.

Procedure

1 In the software installer directory, double-click the `autorun.exe` file to start the installer.

2 Select **vSphere Web Client** and click **Install**.

3 Follow the prompts in the installation wizard to choose the installer language, and agree to the end user patent and license agreements.

4 Either accept the default destination folder or click **Change** to select another location.

The installation path cannot contain any of the following characters: non-ASCII characters, commas (,), periods (.), exclamation points (!), pound signs (#), at signs (@), or percentage signs (%).

If 8.3 name creation is disabled on the host machine, do not install the vSphere Web Clientin a directory that does not have an 8.3 short name or has a name that contains spaces. This situation will make the vSphere Web Client inaccessible.

5 Accept or change the default port settings.

6 Enter the information to register the vSphere Web Client with vCenter Single Sign-On.

The vCenter Single Sign-On administrator user name is administrator@vsphere.local, and the password must match the password you entered for the administrator user when you installed vCenter Single Sign-On. The Lookup Service URL takes the form https://*SSO_host_FQDN_or_IP*:7444/lookupservice/sdk, where 7444 is the default vCenter Single Sign-On HTTPS port number. Your entry should match the entry you made when you installed vCenter Single Sign-On. If you entered a different port number when you installed vCenter Single Sign-On, use that port number.

7 Click **Install**.

8 Start the vSphere Web Client by taking one of the following actions.

- If you are starting the vSphere Web Client for the first time, open a supported browser, and go to https://*vSphere_Web_Client_host_name_or_IP*:9443/vsphere-client.
- In subsequent sessions, you can start the vSphere Web Client from the Windows Start menu, by selecting **Programs > VMware > VMware vSphere Web Client > vSphere Web Client**.

NOTE After you upgrade the vSphere Web Client, when you log in for the first time, you may see the error message `Failed to navigate to desired location`. This can happen when a vSphere Web Client session from the previous version remains open when you upgrade. In this case, refresh the browser and log in again.

Upgrade vCenter Inventory Service Separately by Using Custom Install

You can use Custom Install to upgrade vCenter Single Sign-On, vCenter Inventory Service, and vCenter Server separately to customize the location and configuration of the components.

These instructions upgrade vCenter Inventory Service only. You must install or upgrade vCenter Single Sign-On before upgrading Inventory Service and vCenter Server.

NOTE vCenter Server 5.5 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPv4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

Prerequisites

- Review "vCenter Single Sign-On Deployment Modes," on page 33.
- Review "How vCenter Single Sign-On Affects vCenter Server Upgrades," on page 32.

- See "Prerequisites for the vCenter Server Upgrade," on page 48
- Download the vCenter Server Installer.
- Upgrade vCenter Single Sign-On.

Procedure

1. In the software installer directory, double-click the `autorun.exe` file to start the installer.
2. Select **vCenter Inventory Service** and click **Install.**
3. Follow the prompts in the installation wizard to choose the installer language, and agree to the end user patent and license agreements.
4. If you are upgrading or reinstalling an existing instance of Inventory Service, choose whether to keep the existing database or replace it with a new empty database.
5. Click **Install**.

Inventory Service is upgraded.

Upgrade vCenter Server Separately by Using Custom Install

You can upgrade vCenter Server separately after installing vCenter Single Sign-On, and upgrading Inventory Service.

Alternatively, you can upgrade vCenter Server as part of a Simple Install. See "Use Simple Install to Upgrade vCenter Server and Required Components," on page 65 and "How vCenter Single Sign-On Affects vCenter Server Upgrades," on page 32.

This procedure requires downtime for the vCenter Server that you are upgrading. You do not need to turn off virtual machines.

If an earlier version of vCenter Server is on your machine, the vCenter Server installer detects and upgrades it. If the upgrade fails, no automatic rollback occurs to the previous vCenter Server version.

NOTE vCenter Server 5.5 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPv4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

Prerequisites

- Review "vCenter Single Sign-On Deployment Modes," on page 33.
- Review "How vCenter Single Sign-On Affects vCenter Server Upgrades," on page 32.
- See "Prerequisites for the vCenter Server Upgrade," on page 48
- Install vCenter Single Sign-On and Inventory Service.

Procedure

1. In the software installer directory, double-click the `autorun.exe` file to start the installer.
2. Select **vCenter Server** and click **Install**.
3. Follow the prompts in the installation wizard to choose the installer language, and agree to the end user patent and license agreements.
4. Enter or confirm your database credentials.

5 Select whether to upgrade the vCenter Server database.

- Select **Upgrade existing vCenter Server database** to continue with the upgrade to vCenter Server.
- Select **Do not upgrade existing vCenter Server database** if you do not have a backup copy of your database.

  You cannot continue the upgrade.

6 Click **I have taken a backup of the existing vCenter Server database and SSL certificates**.

7 Select how to upgrade vCenter Agent.

Option	Description
Automatic	To automatically upgrade vCenter Agent on all the hosts in the vCenter Server inventory.
Manual	If one of the following applies: ■ You need to control the timing of vCenter Agent upgrades on specific hosts. ■ vCenter Agent is installed on each host in the inventory to enable vCenter Server to manage the host. vCenter Agent must be upgraded when vCenter Server is upgraded.

vCenter Agent is installed on each host in the inventory to enable vCenter Server to manage the host. vCenter Agent must be upgraded when vCenter Server is upgraded.

8 Select the account for the vCenter Service to run in.

Option	Description
SYSTEM Account	Select the **Use Windows Local System Account** check box, type the fully qualified domain name of the vCenter Server host, and click **Next**. You cannot use the Use Windows Local System Account account if you are using the bundled database or SQL Server with Windows authentication.
User-specified account	Deselect the **Use Windows Local System Account** check box, type the account password and the fully qualified domain name of the vCenter Server host, and click **Next**.

9 Accept or change the port numbers to connect to vCenter Server.

10 (Optional) Select **Increase the number of available ephemeral ports**.

11 Select the size of your vCenter Server inventory to allocate memory for several Java services that are used by vCenter Server.

This setting determines the maximum JVM heap settings for VMware VirtualCenter Management Webservices (Tomcat), Inventory Service, and Profile-Driven Storage Service. You can adjust this setting after installation if the number of hosts in your environment changes. See the recommendations in the topic vCenter Server Hardware Requirements.

12 Enter the information to register vCenter Server with vCenter Single Sign-On.

The vCenter Single Sign-On administrator user name is administrator@vsphere.local, and the password must match the password you entered when you installed vCenter Single Sign-On. The Lookup Service URL takes the form https://*SSO_host_FQDN_or_IP*:7444/lookupservice/sdk, where 7444 is the default vCenter Single Sign-On HTTPS port number. Your entry should match the entry you made when you installed vCenter Single Sign-On. If you entered a different port number when you installed vCenter Single Sign-On, use that port number.

NOTE If you installed vCenter Single Sign-On in a vCenter Server Appliance, you can enter the vCenter Single Sign-On administrator user as root@localos. In this case, the password is the root password of the vCenter Server Appliance. The Lookup Service URL takes the form https://*vCenter_Appliance_IP_or_host_name*:{7444}/lookupservice/sdk.

13 Enter the Inventory Service URL.

The Inventory Service URL takes the form https://*Inventory_Service_host_FQDN_or_IP*:10443. 10443 is the default Inventory Service HTTPS port number. If you entered a different port number when you installed Inventory Service, use that port number here.

14 Click **Install**.

Installation might take several minutes. Multiple progress bars appear during the installation of the selected components.

What to do next

Review the topics in Chapter 5, "After You Upgrade vCenter Server," on page 127 for other postupgrade actions you might want to take.

Use Custom Install to Upgrade vCenter Server from a Version 5.1.x High Availability vCenter Single Sign-On Deployment

In high availability mode, two vCenter Single Sign-On nodes work with the same database, data, and user stores to ensure that vCenter Single Sign-On is not a single point of failure.

This procedure upgrades an existing vCenter Server that was installed with a high availability vCenter Single Sign-On deployment.

You can upgrade vCenter Single Sign-On in a high availability installation without taking all vCenter Single Sign-On nodes offline at the same time. While the first Single Sign-On node is being upgraded, the load balancer will redirect all requests to the second node. After the first node is successfully upgraded, you can upgrade the second node.

vCenter Server can continue running while you upgrade vCenter Single Sign-On. Logged in users can continue accessing vCenter Server and related solutions that are connected to vCenter Single Sign-On during the upgrade. However, vCenter Server, the vSphere Web Client, and vCenter Inventory Service cannot be started while the first Single Sign-On node is offline.

NOTE vCenter Server 5.5 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPv4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

Prerequisites

- Review the topics in Chapter 3, "Preparing for the Upgrade to vCenter Server," on page 31.
- See "Prerequisites for the vCenter Server Upgrade," on page 48

- Verify that the load balancer in your existing vCenter Single Sign-On high availability deployment is configured as described in VMware Knowledge Base articles 2034157 and 2033588 .

Procedure

1 Upgrade the First vCenter Single Sign-On Node in a High Availability Installation on page 85

Upgrade the first node in a vCenter Single Sign-On installation for high availability.

2 Upgrade an Additional vCenter Single Sign-On Server for High Availability on page 86

Upgrade an additional vCenter Single Sign-On node for an existing high availability vCenter Single Sign-On installation.

3 Reconfigure the Load Balancer After Upgrading a vCenter Single Sign-On High Availability Deployment to Version 5.5 on page 87

After you upgrade both nodes of a 5.1.x vCenter Single Sign-On high availability deployment to version 5.5, reconfigure the load balancer.

4 Install or Upgrade the vSphere Web Client on page 89

The vSphere Web Client lets you connect to a vCenter Server system to manage your vSphere deployment through a browser.

5 Upgrade vCenter Inventory Service Separately by Using Custom Install on page 90

You can use Custom Install to upgrade vCenter Single Sign-On, vCenter Inventory Service, and vCenter Server separately to customize the location and configuration of the components.

6 Upgrade vCenter Server Separately by Using Custom Install on page 91

You can upgrade vCenter Server separately after installing vCenter Single Sign-On, and upgrading Inventory Service.

Upgrade the First vCenter Single Sign-On Node in a High Availability Installation

Upgrade the first node in a vCenter Single Sign-On installation for high availability.

NOTE vCenter Server 5.5 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPv4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

For more information about vCenter Single Sign-On, see "How vCenter Single Sign-On Affects vCenter Server Upgrades," on page 32 and the *vSphere Security* documentation.

Prerequisites

- Review Prerequisites for the vCenter Server Upgrade.

Procedure

1 In the software installer directory, double-click the `autorun.exe` file to start the installer.

2 Select **vCenter Single Sign-On** and click **Install**.

3 Follow the prompts in the installation wizard to choose the installer language, and agree to the end user patent and license agreements.

4 Enter the password for the vCenter Single Sign-On administrator account.

5 Click **Install.**

The first high availability vCenter Single Sign-On node is upgraded.

After vCenter Single Sign-On is installed or upgraded, the following default identity sources and users are available:

localos	All local operating system users. These users can be granted permissions to vCenter Server. If you are upgrading, those users who already have permissions keep those permissions.
vsphere.local	Contains all users who have administrator access to the vCenter Single Sign-On server. Initially, only the user administrator is defined.

To add other identity sources, such as a native Active Directory (Integrated Windows Authentication) domain or an OpenLDAP directory service, see "Add a vCenter Single Sign-On Identity Source," on page 104.

What to do next

Upgrade the second vCenter Single Sign-On instance. See "Upgrade an Additional vCenter Single Sign-On Server for High Availability," on page 86.

Upgrade an Additional vCenter Single Sign-On Server for High Availability

Upgrade an additional vCenter Single Sign-On node for an existing high availability vCenter Single Sign-On installation.

Prerequisites

See the previous steps in this multitask topic, "Use Custom Install to Upgrade vCenter Server from a Version 5.1.x High Availability vCenter Single Sign-On Deployment," on page 84

Procedure

1 In the software installer directory, double-click the `autorun.exe` file to start the installer.

2 Select **vCenter Single Sign-On** and click **Install**.

3 Follow the prompts in the installation wizard to choose the installer language, and agree to the end user patent and license agreements.

4 Enter the password for the vCenter Single Sign-On administrator account.

5 Accept or change the HTTPS port for vCenter Single Sign-On.

6 Select the deployment mode **Additional server in an existing domain**.

7 Enter the information to point this additional node to the first vCenter Single Sign-On server.

NOTE If the primary node is in a high-availability cluster, enter the address of the primary node load balancer.

   a Enter the **Partner host name**.

   The partner host name is the DNS name of the existing vCenter Single Sign-On server to replicate from.

   b Enter the password for the vCenter Single Sign-On administrator account of the existing vCenter Single Sign-On server (administrator@vsphere.local).

8 Select an existing site as the partner or enter a new site.

9 Click **Install**.

Reconfigure the Load Balancer After Upgrading a vCenter Single Sign-On High Availability Deployment to Version 5.5

After you upgrade both nodes of a 5.1.x vCenter Single Sign-On high availability deployment to version 5.5, reconfigure the load balancer.

Prerequisites

Upgrade both vCenter Single Sign-On nodes to version 5.5.

Procedure

1 In the `httpd.conf` file of the load balancer, in the section `Configure the STS for clustering`, change values from `ims` to `sts`.

Use the following example as a model.

```
# Configure the STS for clustering
 ProxyPass /sts/ balancer://stscluster/ nofailover=On
 ProxyPassReverse /sts/ balancer://stscluster/

 Header add Set-Cookie "ROUTEID=.%{BALANCER_WORKER_ROUTE}e; path=/sts"
env=BALANCER_ROUTE_CHANGED
 <Proxy balancer://stscluster>
   BalancerMember https://sso1.example.com:7444/sts route=node1 loadfactor=100 retry=300
   BalancerMember https://sso2.example.com:7444/sts route=node2 loadfactor=1 retry=300
   ProxySet lbmethod=byrequests stickysession=ROUTEID failonstatus=500
 </Proxy>
```

2 Configure both vCenter Single Sign-On servers for load balancing.

a In the first vCenter Single Sign-On node, edit the file `server.xml` to add the entry `jvmRoute="node1"`.

The default location of the file is `C:\ProgramData\VMware\cis\runtime\VMwareSTService\conf\server.xml`.

b Restart TC server.

c In the second vCenter Single Sign-On node, edit the file `server.xml` to add the entry `jvmRoute="node2"`.

The default location of the file is `C:\ProgramData\VMware\cis\runtime\VMwareSTService\conf\server.xml`.

d Restart TC server.

3 In the first vCenter Single Sign-On node, take the following actions:

a From a command prompt, run `ssolscli.cmd listServices` to get the service endpoints.

b Edit the files `sts_id`, `admin_id`, and `gc_id` to match the ServerId's from the output of the `ssolscli.cmd listServices` command.

Each file should contains single line similar to:

`SSO node1 Site name``:a03772af-b7db-4629-ac88-ba677516e2b1`

4 Edit the file `sts.properties` to replace the vCenter Single Sign-On hostname with the load balancer hostname.

Use the following example as a model:

```
[service]
friendlyName=The security token service interface of the SSO server
version=1.5
ownerId=
type=urn:sso:sts
description=The security token service interface of the SSO server
productId=product:sso
viSite=SSO node1 site name

[endpoint0]
uri=https://loadbalancer fqdn.com:7444/sts/STSService/vsphere.local
ssl=C:\updateInfo\cacert.pem
protocol=wsTrust
```

5 Edit the file `admin.properties` to replace the vCenter Single Sign-On hostname with the load balancer hostname.

Use the following example as a model:

```
[service]
friendlyName=The administrative interface of the SSO server
version=1.5
ownerId=
type=urn:sso:admin
description=The administrative interface of the SSO server
productId=product:sso
viSite=SSO node1 site name

[endpoint0]
uri=https://loadbalancer fqdn.com:7444/sso-adminserver/sdk/vsphere.local
ssl=C:\updateInfo\cacert.pem
protocol=vmomi
```

6 Edit the file `gc.properties` to replace the vCenter Single Sign-On hostname with the load balancer hostname.

Use the following example as a model:

```
[service]
friendlyName=The group check interface of the SSO server
version=1.5
ownerId=
type=urn:sso:groupcheck
description=The group check interface of the SSO server
productId=product:sso
viSite=SSO node1 site name

[endpoint0]
uri=https://loadbalancer fqdn.com:7444/sso-adminserver/sdk/vsphere.local
ssl=C:\updateInfo\cacert.pem
protocol=vmomi
```

7 For each of the service ID, run the command `ssolscli.cmd updateService`:

```
ssolscli.cmd updateService –d https://sso1.example.com/lookupservice/sdk –u
Administrator@vsphere.local –p password –si sts_id –ip sts.properties
ssolscli.cmd updateService –d https://sso1.example.com/lookupservice/sdk –u
Administrator@vsphere.local –p password –si admin_id –ip admin.properties
ssolscli.cmd updateService –d https://sso1.example.com/lookupservice/sdk –u
Administrator@vsphere.local –p password –si gc_id –ip gc.properties
```

8 Restart the first vCenter Single Sign-On node.

9 Restart the second vCenter Single Sign-On node.

10 Restart the load balancer.

What to do next

Upgrade the vSphere Web Client.

Install or Upgrade the vSphere Web Client

The vSphere Web Client lets you connect to a vCenter Server system to manage your vSphere deployment through a browser.

If an earlier version of the vSphere Web Client is installed, this procedure upgrades the vSphere Web Client.

NOTE vCenter Server 5.5 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPv4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

Prerequisites

- Download the vCenter Server installer. See "Download the vCenter Server Installer," on page 59.
- Verify that the system has an Internet connection.
- Verify that the system meets the software requirements for the vSphere Web Client. See "vSphere Web Client Software Requirements," on page 22.
- Before you install or upgrade any vSphere product, synchronize the clocks of all machines on the vSphere network. See "Synchronizing Clocks on the vSphere Network," on page 53.
- Install vCenter Single Sign-On, or upgrade to the current version.
- Verify that the vSphere Web Client and vCenter Server are registered to the same vCenter Single Sign-On server, to ensure that the vSphere Web Client can access the vCenter Server inventory.
- Close all browsers before installing or uninstalling the vSphere Web Client.
- Log in as a member of the Administrators group on the host machine, with a user name that does not contain any non-ASCII characters.

Procedure

1 In the software installer directory, double-click the `autorun.exe` file to start the installer.

2 Select **vSphere Web Client** and click **Install**.

3 Follow the prompts in the installation wizard to choose the installer language, and agree to the end user patent and license agreements.

4 Either accept the default destination folder or click **Change** to select another location.

The installation path cannot contain any of the following characters: non-ASCII characters, commas (,), periods (.), exclamation points (!), pound signs (#), at signs (@), or percentage signs (%).

If 8.3 name creation is disabled on the host machine, do not install the vSphere Web Clientin a directory that does not have an 8.3 short name or has a name that contains spaces. This situation will make the vSphere Web Client inaccessible.

5 Accept or change the default port settings.

6 Enter the information to register the vSphere Web Client with vCenter Single Sign-On.

The vCenter Single Sign-On administrator user name is administrator@vsphere.local, and the password must match the password you entered for the administrator user when you installed vCenter Single Sign-On. The Lookup Service URL takes the form https://*SSO_host_FQDN_or_IP*:7444/lookupservice/sdk, where 7444 is the default vCenter Single Sign-On HTTPS port number. Your entry should match the entry you made when you installed vCenter Single Sign-On. If you entered a different port number when you installed vCenter Single Sign-On, use that port number.

7 Click **Install**.

8 Start the vSphere Web Client by taking one of the following actions.

- If you are starting the vSphere Web Client for the first time, open a supported browser, and go to https://*vSphere_Web_Client_host_name_or_IP*:9443/vsphere-client.
- In subsequent sessions, you can start the vSphere Web Client from the Windows Start menu, by selecting **Programs > VMware > VMware vSphere Web Client > vSphere Web Client**.

NOTE After you upgrade the vSphere Web Client, when you log in for the first time, you may see the error message `Failed to navigate to desired location`. This can happen when a vSphere Web Client session from the previous version remains open when you upgrade. In this case, refresh the browser and log in again.

Upgrade vCenter Inventory Service Separately by Using Custom Install

You can use Custom Install to upgrade vCenter Single Sign-On, vCenter Inventory Service, and vCenter Server separately to customize the location and configuration of the components.

These instructions upgrade vCenter Inventory Service only. You must install or upgrade vCenter Single Sign-On before upgrading Inventory Service and vCenter Server.

NOTE vCenter Server 5.5 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPv4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

Prerequisites

- Review "vCenter Single Sign-On Deployment Modes," on page 33.
- Review "How vCenter Single Sign-On Affects vCenter Server Upgrades," on page 32.
- See "Prerequisites for the vCenter Server Upgrade," on page 48
- Download the vCenter Server Installer.
- Upgrade vCenter Single Sign-On.

Procedure

1 In the software installer directory, double-click the `autorun.exe` file to start the installer.

2 Select **vCenter Inventory Service** and click **Install.**

3 Follow the prompts in the installation wizard to choose the installer language, and agree to the end user patent and license agreements.

4 If you are upgrading or reinstalling an existing instance of Inventory Service, choose whether to keep the existing database or replace it with a new empty database.

5 Click **Install**.

Inventory Service is upgraded.

Upgrade vCenter Server Separately by Using Custom Install

You can upgrade vCenter Server separately after installing vCenter Single Sign-On, and upgrading Inventory Service.

Alternatively, you can upgrade vCenter Server as part of a Simple Install. See "Use Simple Install to Upgrade vCenter Server and Required Components," on page 65 and "How vCenter Single Sign-On Affects vCenter Server Upgrades," on page 32.

This procedure requires downtime for the vCenter Server that you are upgrading. You do not need to turn off virtual machines.

If an earlier version of vCenter Server is on your machine, the vCenter Server installer detects and upgrades it. If the upgrade fails, no automatic rollback occurs to the previous vCenter Server version.

NOTE vCenter Server 5.5 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPv4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

Prerequisites

- Review "vCenter Single Sign-On Deployment Modes," on page 33.
- Review "How vCenter Single Sign-On Affects vCenter Server Upgrades," on page 32.
- See "Prerequisites for the vCenter Server Upgrade," on page 48
- Install vCenter Single Sign-On and Inventory Service.

Procedure

1 In the software installer directory, double-click the `autorun.exe` file to start the installer.

2 Select **vCenter Server** and click **Install**.

3 Follow the prompts in the installation wizard to choose the installer language, and agree to the end user patent and license agreements.

4 Enter or confirm your database credentials.

5 Select whether to upgrade the vCenter Server database.

- Select **Upgrade existing vCenter Server database** to continue with the upgrade to vCenter Server.
- Select **Do not upgrade existing vCenter Server database** if you do not have a backup copy of your database.

  You cannot continue the upgrade.

6 Click **I have taken a backup of the existing vCenter Server database and SSL certificates**.

7 Select how to upgrade vCenter Agent.

Option	Description
Automatic	To automatically upgrade vCenter Agent on all the hosts in the vCenter Server inventory.
Manual	If one of the following applies: ■ You need to control the timing of vCenter Agent upgrades on specific hosts. ■ vCenter Agent is installed on each host in the inventory to enable vCenter Server to manage the host. vCenter Agent must be upgraded when vCenter Server is upgraded.

vCenter Agent is installed on each host in the inventory to enable vCenter Server to manage the host. vCenter Agent must be upgraded when vCenter Server is upgraded.

8 Select the account for the vCenter Service to run in.

Option	Description
SYSTEM Account	Select the **Use Windows Local System Account** check box, type the fully qualified domain name of the vCenter Server host, and click **Next**. You cannot use the Use Windows Local System Account account if you are using the bundled database or SQL Server with Windows authentication.
User-specified account	Deselect the **Use Windows Local System Account** check box, type the account password and the fully qualified domain name of the vCenter Server host, and click **Next**.

9 Accept or change the port numbers to connect to vCenter Server.

10 (Optional) Select **Increase the number of available ephemeral ports**.

11 Select the size of your vCenter Server inventory to allocate memory for several Java services that are used by vCenter Server.

This setting determines the maximum JVM heap settings for VMware VirtualCenter Management Webservices (Tomcat), Inventory Service, and Profile-Driven Storage Service. You can adjust this setting after installation if the number of hosts in your environment changes. See the recommendations in the topic vCenter Server Hardware Requirements.

12 Enter the information to register vCenter Server with vCenter Single Sign-On.

The vCenter Single Sign-On administrator user name is administrator@vsphere.local, and the password must match the password you entered when you installed vCenter Single Sign-On. The Lookup Service URL takes the form https://*SSO_host_FQDN_or_IP*:7444/lookupservice/sdk, where 7444 is the default vCenter Single Sign-On HTTPS port number. Your entry should match the entry you made when you installed vCenter Single Sign-On. If you entered a different port number when you installed vCenter Single Sign-On, use that port number.

NOTE If you installed vCenter Single Sign-On in a vCenter Server Appliance, you can enter the vCenter Single Sign-On administrator user as root@localos. In this case, the password is the root password of the vCenter Server Appliance. The Lookup Service URL takes the form https://*vCenter_Appliance_IP_or_host_name*:{7444}/lookupservice/sdk.

13 Enter the Inventory Service URL.

The Inventory Service URL takes the form https://*Inventory_Service_host_FQDN_or_IP*:10443. 10443 is the default Inventory Service HTTPS port number. If you entered a different port number when you installed Inventory Service, use that port number here.

14 Click **Install**.

Installation might take several minutes. Multiple progress bars appear during the installation of the selected components.

What to do next

Review the topics in Chapter 5, "After You Upgrade vCenter Server," on page 127 for other postupgrade actions you might want to take.

Use Custom Install to Upgrade vCenter Server from a Version 5.1.x Multisite vCenter Single Sign-On Deployment

The vCenter Server 5.1.x multisite deployment enables a single administrator to administer vCenter Server instances that are deployed on geographically dispersed sites in Linked Mode. when you upgrade to vCenter Server 5.5, the vCenter Single Sign-On deployment changes.

In vCenter Server 5.5, each vCenter Single Sign-On instance uses the default identity source, and can use other identity sources if the domain is included when a user logs in.

There are no components in the vSphere suite that communicate with multiple vCenter Single Sign-On servers. Each vSphere component should be configured to communicate with its local vCenter Single Sign-On instance for faster access.

NOTE vCenter Server 5.5 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPv4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

Prerequisites

- Review the topics in Chapter 3, "Preparing for the Upgrade to vCenter Server," on page 31.
- See "Prerequisites for the vCenter Server Upgrade," on page 48
- When you upgrade from an existing multisite Single Sign-On deployment of vCenter Server, to maintain Linked Mode functionality you must upgrade all Single Sign-On instances to the same version and manually resynchronize all Single Sign-On instances. See Knowledge Base articles http://kb.vmware.com/kb/2042849 and http://kb.vmware.com/kb/2038677.

Procedure

1 Install or Upgrade the First vCenter Single Sign-On Server in a Multisite vCenter Single Sign-On Installation on page 94

Create or upgrade the first vCenter Single Sign-On server for a multisite vCenter Single Sign-On installation.

2 Install or Upgrade the vSphere Web Client on page 95

The vSphere Web Client lets you connect to a vCenter Server system to manage your vSphere deployment through a browser.

3 Upgrade vCenter Inventory Service Separately by Using Custom Install on page 96

You can use Custom Install to upgrade vCenter Single Sign-On, vCenter Inventory Service, and vCenter Server separately to customize the location and configuration of the components.

4 Upgrade vCenter Server Separately by Using Custom Install on page 97

You can upgrade vCenter Server separately after installing vCenter Single Sign-On, and upgrading Inventory Service.

5 Install or Upgrade an Additional Single Sign-On Server for a Multisite vCenter Single Sign-On Installation on page 99

Create or upgrade an additional vCenter Single Sign-On server for a multisite vCenter Single Sign-On installation.

6 Install or Upgrade the vSphere Web Client on page 100

The vSphere Web Client lets you connect to a vCenter Server system to manage your vSphere deployment through a browser.

7 Upgrade vCenter Inventory Service Separately by Using Custom Install on page 101

You can use Custom Install to upgrade vCenter Single Sign-On, vCenter Inventory Service, and vCenter Server separately to customize the location and configuration of the components.

8 Upgrade vCenter Server Separately by Using Custom Install on page 102

You can upgrade vCenter Server separately after installing vCenter Single Sign-On, and upgrading Inventory Service.

Install or Upgrade the First vCenter Single Sign-On Server in a Multisite vCenter Single Sign-On Installation

Create or upgrade the first vCenter Single Sign-On server for a multisite vCenter Single Sign-On installation.

Prerequisites

- Review "vCenter Single Sign-On Deployment Modes," on page 33.
- Review "How vCenter Single Sign-On Affects vCenter Server Upgrades," on page 32.
- See "Prerequisites for the vCenter Server Upgrade," on page 48

Procedure

1 In the software installer directory, double-click the `autorun.exe` file to start the installer.

2 Select **vCenter Single Sign-On** and click **Install**.

3 Follow the prompts in the installation wizard to choose the installer language, and agree to the end user patent and license agreements.

4 If you are installing a new instance of vCenter Single Sign-On , proceed to Step 5. If you are upgrading an existing installation of vCenter Single Sign-On , take the following steps:

a Enter the password for the vCenter Single Sign-On administrator account.

b Proceed to Step 8.

5 Accept or change the HTTPS port for vCenter Single Sign-On.

6 Select the deployment mode **vCenter Single Sign-On for your first vCenter Server**.

7 Set the password for the vCenter Single Sign-On administrator account.

This is the password for the user administrator@vsphere.local. vsphere.local is a new domain that is created by vCenter Single Sign-On. After installation, you can log in to vCenter Single Sign-On and in to vCenter Server as adminstrator@vsphere.local.

By default, the password must have at least eight characters, at least one lowercase character, one uppercase character, one number, and one special character. See the *vSphere Security* documentation for information about changing the password policy. The following characters are not supported in passwords: non-ASCII characters, semicolon (;), double quotation mark ("), single quotation mark ('), circumflex (^), and backslash (\).

8 Review the installation options and click **Install.**

The first vCenter Single Sign-On multisite server is installed or upgraded.

After vCenter Single Sign-On is installed or upgraded, the following default identity sources and users are available:

localos	All local operating system users. These users can be granted permissions to vCenter Server. If you are upgrading, those users who already have permissions keep those permissions.
vsphere.local	Contains all users who have administrator access to the vCenter Single Sign-On server. Initially, only the user administrator is defined.

To add other identity sources, such as a native Active Directory (Integrated Windows Authentication) domain or an OpenLDAP directory service, see "Add a vCenter Single Sign-On Identity Source," on page 104.

Install or Upgrade the vSphere Web Client

The vSphere Web Client lets you connect to a vCenter Server system to manage your vSphere deployment through a browser.

If an earlier version of the vSphere Web Client is installed, this procedure upgrades the vSphere Web Client.

NOTE vCenter Server 5.5 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPv4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

Prerequisites

- Download the vCenter Server installer. See "Download the vCenter Server Installer," on page 59.
- Verify that the system has an Internet connection.
- Verify that the system meets the software requirements for the vSphere Web Client. See "vSphere Web Client Software Requirements," on page 22.
- Before you install or upgrade any vSphere product, synchronize the clocks of all machines on the vSphere network. See "Synchronizing Clocks on the vSphere Network," on page 53.
- Install vCenter Single Sign-On, or upgrade to the current version.
- Verify that the vSphere Web Client and vCenter Server are registered to the same vCenter Single Sign-On server, to ensure that the vSphere Web Client can access the vCenter Server inventory.
- Close all browsers before installing or uninstalling the vSphere Web Client.
- Log in as a member of the Administrators group on the host machine, with a user name that does not contain any non-ASCII characters.

Procedure

1. In the software installer directory, double-click the `autorun.exe` file to start the installer.
2. Select **vSphere Web Client** and click **Install**.
3. Follow the prompts in the installation wizard to choose the installer language, and agree to the end user patent and license agreements.
4. Either accept the default destination folder or click **Change** to select another location.

   The installation path cannot contain any of the following characters: non-ASCII characters, commas (,), periods (.), exclamation points (!), pound signs (#), at signs (@), or percentage signs (%).

If 8.3 name creation is disabled on the host machine, do not install the vSphere Web Clientin a directory that does not have an 8.3 short name or has a name that contains spaces. This situation will make the vSphere Web Client inaccessible.

5 Accept or change the default port settings.

6 Enter the information to register the vSphere Web Client with vCenter Single Sign-On.

The vCenter Single Sign-On administrator user name is administrator@vsphere.local, and the password must match the password you entered for the administrator user when you installed vCenter Single Sign-On. The Lookup Service URL takes the form https://*SSO_host_FQDN_or_IP*:7444/lookupservice/sdk, where 7444 is the default vCenter Single Sign-On HTTPS port number. Your entry should match the entry you made when you installed vCenter Single Sign-On. If you entered a different port number when you installed vCenter Single Sign-On, use that port number.

7 Click **Install**.

8 Start the vSphere Web Client by taking one of the following actions.

- If you are starting the vSphere Web Client for the first time, open a supported browser, and go to https://*vSphere_Web_Client_host_name_or_IP*:9443/vsphere-client.
- In subsequent sessions, you can start the vSphere Web Client from the Windows Start menu, by selecting **Programs > VMware > VMware vSphere Web Client > vSphere Web Client**.

NOTE After you upgrade the vSphere Web Client, when you log in for the first time, you may see the error message `Failed to navigate to desired location`. This can happen when a vSphere Web Client session from the previous version remains open when you upgrade. In this case, refresh the browser and log in again.

Upgrade vCenter Inventory Service Separately by Using Custom Install

You can use Custom Install to upgrade vCenter Single Sign-On, vCenter Inventory Service, and vCenter Server separately to customize the location and configuration of the components.

These instructions upgrade vCenter Inventory Service only. You must install or upgrade vCenter Single Sign-On before upgrading Inventory Service and vCenter Server.

NOTE vCenter Server 5.5 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPv4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

Prerequisites

- Review "vCenter Single Sign-On Deployment Modes," on page 33.
- Review "How vCenter Single Sign-On Affects vCenter Server Upgrades," on page 32.
- See "Prerequisites for the vCenter Server Upgrade," on page 48
- Download the vCenter Server Installer.
- Upgrade vCenter Single Sign-On.

Procedure

1 In the software installer directory, double-click the `autorun.exe` file to start the installer.

2 Select **vCenter Inventory Service** and click **Install.**

3 Follow the prompts in the installation wizard to choose the installer language, and agree to the end user patent and license agreements.

4 If you are upgrading or reinstalling an existing instance of Inventory Service, choose whether to keep the existing database or replace it with a new empty database.

5 Click **Install**.

Inventory Service is upgraded.

Upgrade vCenter Server Separately by Using Custom Install

You can upgrade vCenter Server separately after installing vCenter Single Sign-On, and upgrading Inventory Service.

Alternatively, you can upgrade vCenter Server as part of a Simple Install. See "Use Simple Install to Upgrade vCenter Server and Required Components," on page 65 and "How vCenter Single Sign-On Affects vCenter Server Upgrades," on page 32.

This procedure requires downtime for the vCenter Server that you are upgrading. You do not need to turn off virtual machines.

If an earlier version of vCenter Server is on your machine, the vCenter Server installer detects and upgrades it. If the upgrade fails, no automatic rollback occurs to the previous vCenter Server version.

NOTE vCenter Server 5.5 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPv4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

Prerequisites

- Review "vCenter Single Sign-On Deployment Modes," on page 33.
- Review "How vCenter Single Sign-On Affects vCenter Server Upgrades," on page 32.
- See "Prerequisites for the vCenter Server Upgrade," on page 48
- Install vCenter Single Sign-On and Inventory Service.

Procedure

1 In the software installer directory, double-click the `autorun.exe` file to start the installer.

2 Select **vCenter Server** and click **Install**.

3 Follow the prompts in the installation wizard to choose the installer language, and agree to the end user patent and license agreements.

4 Enter or confirm your database credentials.

5 Select whether to upgrade the vCenter Server database.

- Select **Upgrade existing vCenter Server database** to continue with the upgrade to vCenter Server.
- Select **Do not upgrade existing vCenter Server database** if you do not have a backup copy of your database.

  You cannot continue the upgrade.

6 Click **I have taken a backup of the existing vCenter Server database and SSL certificates**.

7 Select how to upgrade vCenter Agent.

Option	Description
Automatic	To automatically upgrade vCenter Agent on all the hosts in the vCenter Server inventory.
Manual	If one of the following applies: ■ You need to control the timing of vCenter Agent upgrades on specific hosts. ■ vCenter Agent is installed on each host in the inventory to enable vCenter Server to manage the host. vCenter Agent must be upgraded when vCenter Server is upgraded.

vCenter Agent is installed on each host in the inventory to enable vCenter Server to manage the host. vCenter Agent must be upgraded when vCenter Server is upgraded.

8 Select the account for the vCenter Service to run in.

Option	Description
SYSTEM Account	Select the **Use Windows Local System Account** check box, type the fully qualified domain name of the vCenter Server host, and click **Next**. You cannot use the Use Windows Local System Account account if you are using the bundled database or SQL Server with Windows authentication.
User-specified account	Deselect the **Use Windows Local System Account** check box, type the account password and the fully qualified domain name of the vCenter Server host, and click **Next**.

9 Accept or change the port numbers to connect to vCenter Server.

10 (Optional) Select **Increase the number of available ephemeral ports**.

11 Select the size of your vCenter Server inventory to allocate memory for several Java services that are used by vCenter Server.

This setting determines the maximum JVM heap settings for VMware VirtualCenter Management Webservices (Tomcat), Inventory Service, and Profile-Driven Storage Service. You can adjust this setting after installation if the number of hosts in your environment changes. See the recommendations in the topic vCenter Server Hardware Requirements.

12 Enter the information to register vCenter Server with vCenter Single Sign-On.

The vCenter Single Sign-On administrator user name is administrator@vsphere.local, and the password must match the password you entered when you installed vCenter Single Sign-On. The Lookup Service URL takes the form https://*SSO_host_FQDN_or_IP*:7444/lookupservice/sdk, where 7444 is the default vCenter Single Sign-On HTTPS port number. Your entry should match the entry you made when you installed vCenter Single Sign-On. If you entered a different port number when you installed vCenter Single Sign-On, use that port number.

NOTE If you installed vCenter Single Sign-On in a vCenter Server Appliance, you can enter the vCenter Single Sign-On administrator user as root@localos. In this case, the password is the root password of the vCenter Server Appliance. The Lookup Service URL takes the form https://*vCenter_Appliance_IP_or_host_name*:{7444}/lookupservice/sdk.

13 Enter the Inventory Service URL.

The Inventory Service URL takes the form https://*Inventory_Service_host_FQDN_or_IP*:10443. 10443 is the default Inventory Service HTTPS port number. If you entered a different port number when you installed Inventory Service, use that port number here.

14 Click **Install**.

Installation might take several minutes. Multiple progress bars appear during the installation of the selected components.

What to do next

Review the topics in Chapter 5, "After You Upgrade vCenter Server," on page 127 for other postupgrade actions you might want to take.

Install or Upgrade an Additional Single Sign-On Server for a Multisite vCenter Single Sign-On Installation

Create or upgrade an additional vCenter Single Sign-On server for a multisite vCenter Single Sign-On installation.

Prerequisites

- Install or upgrade the first node in the multisite vCenter Single Sign-On installation. See "Install or Upgrade the First vCenter Single Sign-On Server in a Multisite vCenter Single Sign-On Installation," on page 94.
- Review "vCenter Single Sign-On Deployment Modes," on page 33.
- See "Prerequisites for the vCenter Server Upgrade," on page 48.

Procedure

1 In the software installer directory, double-click the `autorun.exe` file to start the installer.

2 Select **vCenter Single Sign-On** and click **Install**.

3 Follow the prompts in the installation wizard to choose the installer language, and agree to the end user patent and license agreements.

4 If you are installing a new instance of Single Sign-On, proceed to Step 5. If you are upgrading an existing installation of Single Sign-On, take the following steps:

   a Enter the password for the Single Sign-On administrator account.

   b Proceed to Step 9.

5 Accept or change the HTTPS port for vCenter Single Sign-On.

6 Select the deployment mode **vCenter Single Sign-On for an additional vCenter Server with a new site**.

7 Enter the information to point this additional node to the first vCenter Single Sign-On server.

   NOTE If the primary node is in a high-availability cluster, enter the address of the primary node load balancer.

   a Enter the **Partner host name**.

   The partner host name is the DNS name of the existing vCenter Single Sign-On server to replicate from.

   b Enter the password for the vCenter Single Sign-On administrator account of the existing vCenter Single Sign-On server (administrator@vsphere.local).

8 Select an existing site as the partner or enter a new site.

9 Click **Install.**

The additional vCenter Single Sign-On server is installed.

What to do next

Repeat this procedure for each additional multisite node.

Install or Upgrade the vSphere Web Client

The vSphere Web Client lets you connect to a vCenter Server system to manage your vSphere deployment through a browser.

If an earlier version of the vSphere Web Client is installed, this procedure upgrades the vSphere Web Client.

NOTE vCenter Server 5.5 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPv4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

Prerequisites

- Download the vCenter Server installer. See "Download the vCenter Server Installer," on page 59.
- Verify that the system has an Internet connection.
- Verify that the system meets the software requirements for the vSphere Web Client. See "vSphere Web Client Software Requirements," on page 22.
- Before you install or upgrade any vSphere product, synchronize the clocks of all machines on the vSphere network. See "Synchronizing Clocks on the vSphere Network," on page 53.
- Install vCenter Single Sign-On, or upgrade to the current version.
- Verify that the vSphere Web Client and vCenter Server are registered to the same vCenter Single Sign-On server, to ensure that the vSphere Web Client can access the vCenter Server inventory.
- Close all browsers before installing or uninstalling the vSphere Web Client.
- Log in as a member of the Administrators group on the host machine, with a user name that does not contain any non-ASCII characters.

Procedure

1. In the software installer directory, double-click the `autorun.exe` file to start the installer.
2. Select **vSphere Web Client** and click **Install**.
3. Follow the prompts in the installation wizard to choose the installer language, and agree to the end user patent and license agreements.
4. Either accept the default destination folder or click **Change** to select another location.

   The installation path cannot contain any of the following characters: non-ASCII characters, commas (,), periods (.), exclamation points (!), pound signs (#), at signs (@), or percentage signs (%).

   If 8.3 name creation is disabled on the host machine, do not install the vSphere Web Clientin a directory that does not have an 8.3 short name or has a name that contains spaces. This situation will make the vSphere Web Client inaccessible.
5. Accept or change the default port settings.

6 Enter the information to register the vSphere Web Client with vCenter Single Sign-On.

The vCenter Single Sign-On administrator user name is administrator@vsphere.local, and the password must match the password you entered for the administrator user when you installed vCenter Single Sign-On. The Lookup Service URL takes the form https://*SSO_host_FQDN_or_IP*:7444/lookupservice/sdk, where 7444 is the default vCenter Single Sign-On HTTPS port number. Your entry should match the entry you made when you installed vCenter Single Sign-On. If you entered a different port number when you installed vCenter Single Sign-On, use that port number.

7 Click **Install**.

8 Start the vSphere Web Client by taking one of the following actions.

- If you are starting the vSphere Web Client for the first time, open a supported browser, and go to https://*vSphere_Web_Client_host_name_or_IP*:9443/vsphere-client.
- In subsequent sessions, you can start the vSphere Web Client from the Windows Start menu, by selecting **Programs > VMware > VMware vSphere Web Client > vSphere Web Client**.

NOTE After you upgrade the vSphere Web Client, when you log in for the first time, you may see the error message `Failed to navigate to desired location`. This can happen when a vSphere Web Client session from the previous version remains open when you upgrade. In this case, refresh the browser and log in again.

Upgrade vCenter Inventory Service Separately by Using Custom Install

You can use Custom Install to upgrade vCenter Single Sign-On, vCenter Inventory Service, and vCenter Server separately to customize the location and configuration of the components.

These instructions upgrade vCenter Inventory Service only. You must install or upgrade vCenter Single Sign-On before upgrading Inventory Service and vCenter Server.

NOTE vCenter Server 5.5 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPv4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

Prerequisites

- Review "vCenter Single Sign-On Deployment Modes," on page 33.
- Review "How vCenter Single Sign-On Affects vCenter Server Upgrades," on page 32.
- See "Prerequisites for the vCenter Server Upgrade," on page 48
- Download the vCenter Server Installer.
- Upgrade vCenter Single Sign-On.

Procedure

1 In the software installer directory, double-click the `autorun.exe` file to start the installer.

2 Select **vCenter Inventory Service** and click **Install.**

3 Follow the prompts in the installation wizard to choose the installer language, and agree to the end user patent and license agreements.

4 If you are upgrading or reinstalling an existing instance of Inventory Service, choose whether to keep the existing database or replace it with a new empty database.

5 Click **Install**.

Inventory Service is upgraded.

Upgrade vCenter Server Separately by Using Custom Install

You can upgrade vCenter Server separately after installing vCenter Single Sign-On, and upgrading Inventory Service.

Alternatively, you can upgrade vCenter Server as part of a Simple Install. See "Use Simple Install to Upgrade vCenter Server and Required Components," on page 65 and "How vCenter Single Sign-On Affects vCenter Server Upgrades," on page 32.

This procedure requires downtime for the vCenter Server that you are upgrading. You do not need to turn off virtual machines.

If an earlier version of vCenter Server is on your machine, the vCenter Server installer detects and upgrades it. If the upgrade fails, no automatic rollback occurs to the previous vCenter Server version.

NOTE vCenter Server 5.5 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPv4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

Prerequisites

- Review "vCenter Single Sign-On Deployment Modes," on page 33.
- Review "How vCenter Single Sign-On Affects vCenter Server Upgrades," on page 32.
- See "Prerequisites for the vCenter Server Upgrade," on page 48
- Install vCenter Single Sign-On and Inventory Service.

Procedure

1. In the software installer directory, double-click the `autorun.exe` file to start the installer.
2. Select **vCenter Server** and click **Install**.
3. Follow the prompts in the installation wizard to choose the installer language, and agree to the end user patent and license agreements.
4. Enter or confirm your database credentials.
5. Select whether to upgrade the vCenter Server database.
   - Select **Upgrade existing vCenter Server database** to continue with the upgrade to vCenter Server.
   - Select **Do not upgrade existing vCenter Server database** if you do not have a backup copy of your database.

     You cannot continue the upgrade.
6. Click **I have taken a backup of the existing vCenter Server database and SSL certificates**.

7 Select how to upgrade vCenter Agent.

Option	Description
Automatic	To automatically upgrade vCenter Agent on all the hosts in the vCenter Server inventory.
Manual	If one of the following applies: ■ You need to control the timing of vCenter Agent upgrades on specific hosts. ■ vCenter Agent is installed on each host in the inventory to enable vCenter Server to manage the host. vCenter Agent must be upgraded when vCenter Server is upgraded.

vCenter Agent is installed on each host in the inventory to enable vCenter Server to manage the host. vCenter Agent must be upgraded when vCenter Server is upgraded.

8 Select the account for the vCenter Service to run in.

Option	Description
SYSTEM Account	Select the **Use Windows Local System Account** check box, type the fully qualified domain name of the vCenter Server host, and click **Next**. You cannot use the Use Windows Local System Account account if you are using the bundled database or SQL Server with Windows authentication.
User-specified account	Deselect the **Use Windows Local System Account** check box, type the account password and the fully qualified domain name of the vCenter Server host, and click **Next**.

9 Accept or change the port numbers to connect to vCenter Server.

10 (Optional) Select **Increase the number of available ephemeral ports**.

11 Select the size of your vCenter Server inventory to allocate memory for several Java services that are used by vCenter Server.

This setting determines the maximum JVM heap settings for VMware VirtualCenter Management Webservices (Tomcat), Inventory Service, and Profile-Driven Storage Service. You can adjust this setting after installation if the number of hosts in your environment changes. See the recommendations in the topic vCenter Server Hardware Requirements.

12 Enter the information to register vCenter Server with vCenter Single Sign-On.

The vCenter Single Sign-On administrator user name is administrator@vsphere.local, and the password must match the password you entered when you installed vCenter Single Sign-On. The Lookup Service URL takes the form https://*SSO_host_FQDN_or_IP*:7444/lookupservice/sdk, where 7444 is the default vCenter Single Sign-On HTTPS port number. Your entry should match the entry you made when you installed vCenter Single Sign-On. If you entered a different port number when you installed vCenter Single Sign-On, use that port number.

NOTE If you installed vCenter Single Sign-On in a vCenter Server Appliance, you can enter the vCenter Single Sign-On administrator user as root@localos. In this case, the password is the root password of the vCenter Server Appliance. The Lookup Service URL takes the form https://*vCenter_Appliance_IP_or_host_name*:{7444}/lookupservice/sdk.

13 Enter the Inventory Service URL.

The Inventory Service URL takes the form https://*Inventory_Service_host_FQDN_or_IP*:10443. 10443 is the default Inventory Service HTTPS port number. If you entered a different port number when you installed Inventory Service, use that port number here.

14 Click **Install**.

Installation might take several minutes. Multiple progress bars appear during the installation of the selected components.

What to do next

Review the topics in Chapter 5, "After You Upgrade vCenter Server," on page 127 for other postupgrade actions you might want to take.

Add a vCenter Single Sign-On Identity Source

Users can log in to vCenter Server only if they are in a domain that has been added as a vCenter Single Sign-On identity source. vCenter Single Sign-On administrator users can add identity sources from the vSphere Web Client.

An identity source can be a native Active Directory (Integrated Windows Authentication) domain or an OpenLDAP directory service. For backward compatibility, Active Directory as an LDAP Server is also available.

Immediately after installation, the following default identity sources and users are available:

localos — All local operating system users. These users can be granted permissions to vCenter Server. If you are upgrading, those users who already have permissions keep those permissions.

vsphere.local — Contains the vCenter Single Sign-On internal users.

Procedure

1 Log in to the vSphere Web Client as administrator@vsphere.local or as another user with vCenter Single Sign-On administrator privileges.

2 Browse to **Administration > Single Sign-On > Configuration**.

3 On the **Identity Sources** tab, click the **Add Identity Source** icon.

4 Select the type of identity source and enter the identity source settings.

Option	Description
Active Directory (Integrated Windows Authentication)	Use this option for native Active Directory implementations. See "Active Directory Identity Source Settings," on page 105.
Active Directory as an LDAP Server	This option is available for backward compatibility. It requires that you specify the domain controller and other information. See "Active Directory LDAP Server and OpenLDAP Server Identity Source Settings," on page 105.
OpenLDAP	Use this option for an OpenLDAP identity source. See "Active Directory LDAP Server and OpenLDAP Server Identity Source Settings," on page 105.
LocalOS	Use this option to add the local operating system as an identity source. You are prompted only for the name of the local operating system. If you select this option, all users on the specified machine are visible to vCenter Single Sign-On, even if those users are not part of another domain.

NOTE If the user account is locked or disabled, authentications and group and user searches in the Active Directory domain will fail. The user account must have read-only access over the User and Group OU, and must be able to read user and group attributes. This is the default Active Directory domain configuration for user permissions. VMware recommends using a special service user.

5 If you configured an Active Directory as an LDAP Server or an OpenLDAP identity source, click **Test Connection** to ensure that you can connect to the identity source.

6 Click **OK**.

What to do next

When an identity source is added, all users can be authenticated but have the **No access** permission. A user with vCenter Server **Modify.permissions** privileges can assign permissions to users or groups of users to enable them to log in to vCenter Server. See "Assign Permissions in the vSphere Web Client," on page 106.

Active Directory Identity Source Settings

If you select the Active Directory (Integrated Windows Authentication) identity source type, you can either use the local machine account as your SPN (Service Principal Name) or specify an SPN explicitly.

Select **Use machine account** to speed up configuration. If you expect to rename the local machine on which vCenter Single Sign-On runs, specifying an SPN explicitly is preferable.

Table 4-1. Add Identity Source Settings

Field	Description
Domain name	FDQN of the domain. Do not provide an IP address in this field.
Use machine account	Select this option to use the local machine account as the SPN. When you select this option, you specify only the domain name. Do not select this option if you expect to rename this machine.
Use SPN	Select this option if you expect to rename the local machine. You must specify an SPN, a user who can authenticate with the identity source, and a password for the user.
Service Principal	SPN that helps Kerberos to identify the Active Directory service. Include the domain in the name, for example, STS/example.com. You might have to run `setspn -S` to add the user you want to use. See the Microsoft documentation for information on `setspn`. The SPN must be unique across the domain. Running `setspn -S` checks that no duplicate is created.
User Principal Name	Name of a user who can authenticate with this identity source. Use the email address format, for example, jchin@mydomain.com. You can verify the User Principal Name with the Active Directory Service Interfaces Editor (ADSI Edit).
Password	Password for the user who is used to authenticate with this identity source, which is the user who is specified in User Principal Name. Include the domain name, for example, jdoe@example.com.

Active Directory LDAP Server and OpenLDAP Server Identity Source Settings

The Active Directory as an LDAP Server identity source is available for backward compatibility. Use the Active Directory (Integrated Windows Authentication) option for a setup that requires less input. The OpenLDAP Server identity source is available for environments that use OpenLDAP.

If you are configuring an OpenLDAP identity source, see VMware Knowledge Base article 2064977 for additional requirements.

Table 4-2. Active Directory as an LDAP Server and OpenLDAP Settings

Field	Description
Name	Name of the identity source.
Base DN for users	Base domain name for users.
Domain name	FDQN of the domain, for example, example.com. Do not provide an IP address in this field.
Domain alias	For Active Directory identity sources, the domain's NetBIOS name. Add the NetBIOS name of the Active Directory domain as an alias of the identity source if you are using SSPI authentications. For OpenLDAP identity sources, the domain name in capital letters is added if you do not specify an alias.
Base DN for groups	The base domain name for groups.
Primary Server URL	Primary domain controller LDAP server for the domain. Use the format ldap://hostname:port or ldaps://hostname:port. The port is typically 389 for ldap: connections and 636 for ldaps: connections. For Active Directory multi-domain controller deployments, the port is typically 3268 for ldap: connections and 3269 for ldaps: connections. A certificate that establishes trust for the LDAPS endpoint of the Active Directory server is required when you use ldaps:// in the primary or secondary LDAP URL.
Secondary server URL	Address of a secondary domain controller LDAP server that is used for failover.
Username	ID of a user in the domain who has a minimum of read-only access to Base DN for users and groups.
Password	Password of the user who is specified by Username.

Assign Permissions in the vSphere Web Client

After you create users and groups and define roles, you must assign the users and groups and their roles to the relevant inventory objects. You can assign the same permissions at one time on multiple objects by moving the objects to a folder and setting the permissions on the folder.

Permissions assigned from the vSphere Web Client must match permissions, including case, in ActiveDirectory precisely. If you upgraded from earlier versions of vSphere, check for case inconsistencies if you experience problems with groups.

Prerequisites

Permissions.Modify permission on the parent object of the object whose permissions you want to modify.

Procedure

1 Browse to the object in the vSphere Web Client object navigator.

2 Click the **Manage** tab and select **Permissions**.

3 Click **Add Permission**.

4 Click **Add**.

5 Identify the user or group that will have the permission.

   a Select the domain where the user or group is located from the **Domain** drop-down menu.

   b Type a name in the Search box or select a name from the list.

      The system searches user names, group names, and descriptions.

   c Select the user or group and click **Add**.

      The name is added to either the **Users** or **Groups** list.

   d (Optional) Click **Check Names** to verify that the user or group exists in the database.

   e Click **OK**.

6 Select a role from the **Assigned Role** drop-down menu.

   The roles that are assigned to the object appear in the menu. The privileges contained in the role are listed in the section below the role title.

7 (Optional) Deselect the **Propagate to Child Objects** check box.

   The role is applied only to the selected object and does not propagate to the child objects.

8 Verify that the users and groups are assigned to the appropriate permissions and click **OK**.

   The server adds the permission to the list of permissions for the object.

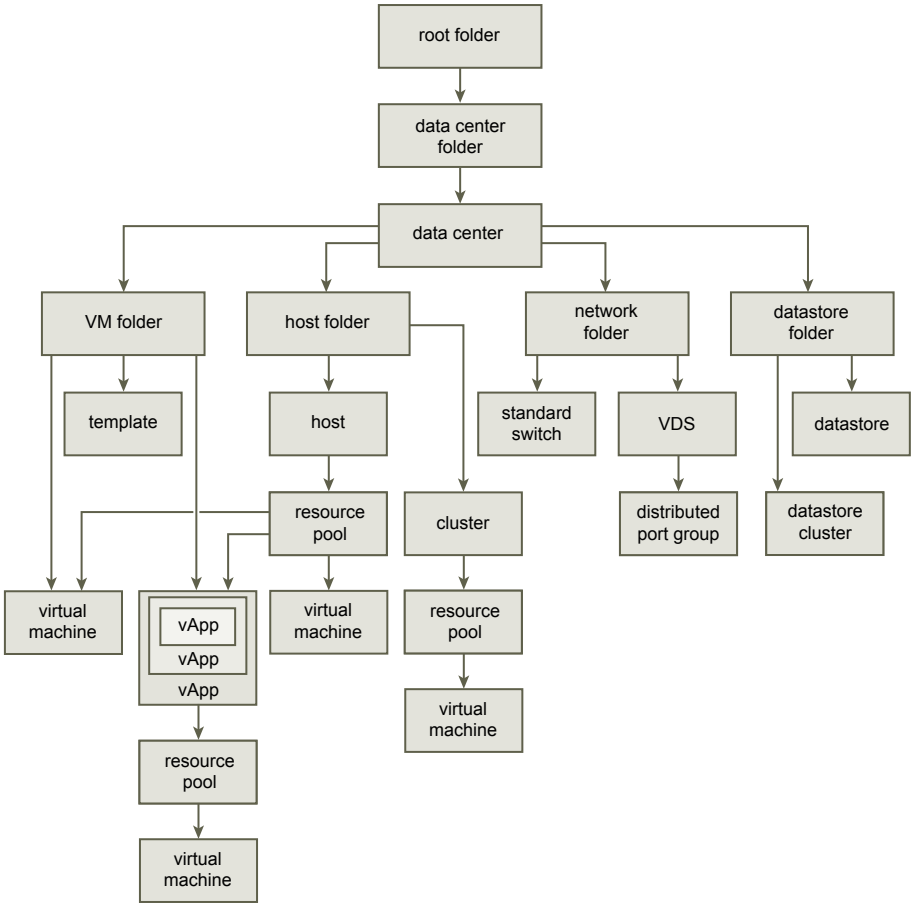
   The list of permissions references all users and groups that have roles assigned to the object and indicates where in the vCenter Server hierarchy the role is assigned.

Hierarchical Inheritance of Permissions

When you assign a permission to an object, you can choose whether the permission propagates down the object hierarchy. You set propagation for each permission. Propagation is not universally applied. Permissions defined for a child object always override the permissions that are propagated from parent objects.

The figure illustrates inventory hierarchy and the paths by which permissions can propagate.

Figure 4-3. vSphere Inventory Hierarchy



Most inventory objects inherit permissions from a single parent object in the hierarchy. For example, a datastore inherits permissions from either its parent datastore folder or parent datacenter. Virtual machines inherit permissions from both the parent virtual machine folder and the parent host, cluster, or resource pool simultaneously. To restrict a user's privileges on a virtual machine, you must set permissions on both the parent folder and the parent host, cluster, or resource pool for that virtual machine.

To set permissions for a distributed switch and its associated distributed port groups, set permissions on a parent object, such a folder or datacenter. You must also select the option to propagate these permissions to child objects.

Permissions take several forms in the hierarchy:

Managed entities You can define permissions on managed entities.

- Clusters
- Datacenters
- Datastores
- Datastore clusters
- Folders
- Hosts
- Networks (except vSphere Distributed Switches)
- Distributed port groups

- Resource pools
- Templates
- Virtual machines
- vSphere vApps

Global entities

Global entities derive permissions from the root vCenter Server system.

- Custom fields
- Licenses
- Roles
- Statistics intervals
- Sessions

Migrate vCenter Server and Components from a Windows Server 2003 Host

vCenter Server 5.5 does not support Windows Server 2003 as a host machine, and does not support upgrades from Windows Server 2003 hosts. You can install vCenter Server 5.5 and related components on a supported host and migrate configuration data from your existing Windows Server 2003 installation.

Prerequisites

- Verify that the new host machine meets the requirements for vCenter Server 5.5. See Chapter 2, "System Requirements," on page 13.
- Review the topics in Chapter 3, "Preparing for the Upgrade to vCenter Server," on page 31.
- Download the vCenter Server installer.

Procedure

1 Install vCenter Single Sign-On in a Migration to vSphere 5.5 from a Windows Server 2003 Host on page 110

vCenter Server 5.5 does not support Windows Server 2003 hosts for vCenter Server. When you migrate from a Windows Server 2003 host to a host that is supported for vCenter Server 5.5, install vCenter Single Sign-On on the new host.

2 Install or Upgrade the vSphere Web Client on page 111

The vSphere Web Client lets you connect to a vCenter Server system to manage your vSphere deployment through a browser.

3 Migrate vSphere Web Client Data from a Windows Server 2003 Host on page 112

When you migrate from a Windows Server 2003 host to a host that is supported for the version 5.5 vCenter Server, you can also migrate some configuration data.

4 Migrate vCenter Inventory Service Data from a Windows Server 2003 Host on page 113

When you migrate from a Windows Server 2003 host to a host that is supported for vCenter Single Sign-On 5.5, you can also migrate Inventory Service SSL certificates and configuration data.

5 Install Inventory Service in a vCenter Server Migration from a Windows Server 2003 Host on page 114

After you migrate Inventory Service SSL certificates and configuration data from a Windows Server 2003 host to a host that is supported for Inventory Service 5.5, you can install Inventory Service on the new host.

6 Migrate vCenter Server Data from a Windows Server 2003 Host on page 115

When you migrate from a Windows Server 2003 host to a host that is supported for vCenter Single Sign-On 5.5, you can also migrate the vCenter Server database and SSL certificates.

7 Install vCenter Server in a Migration from a Windows Server 2003 Host on page 116

After you migrate vCenter Server SSL certificates from a Windows Server 2003 host to a host that is supported for vCenter Server 5.5, you can install vCenter Server on the new host.

Install vCenter Single Sign-On in a Migration to vSphere 5.5 from a Windows Server 2003 Host

vCenter Server 5.5 does not support Windows Server 2003 hosts for vCenter Server. When you migrate from a Windows Server 2003 host to a host that is supported for vCenter Server 5.5, install vCenter Single Sign-On on the new host.

This procedure installs vCenter Single Sign-On in basic mode. To install vCenter Single Sign-On in with multiple instances in the same or different sites, see the *vSphere Installation and Setup* documentation.

NOTE vCenter Server 5.5 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPv4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

Prerequisites

- Review "vCenter Single Sign-On Deployment Modes," on page 33.
- Review "How vCenter Single Sign-On Affects vCenter Server Upgrades," on page 32.
- See "Prerequisites for the vCenter Server Upgrade," on page 48

Procedure

1 In the software installer directory, double-click the `autorun.exe` file to start the installer.

2 Select **vCenter Single Sign-On** and click **Install**.

3 Follow the prompts in the installation wizard to choose the installer language, and agree to the end user patent and license agreements.

4 Accept or change the HTTPS port for vCenter Single Sign-On.

5 Select the deployment mode **vCenter Single Sign-On for your first vCenter Server**.

6 Set the password for the vCenter Single Sign-On administrator account.

This is the password for the user administrator@vsphere.local. vsphere.local is a new domain that is created by vCenter Single Sign-On. After installation, you can log in to vCenter Single Sign-On and in to vCenter Server as adminstrator@vsphere.local.

By default, the password must have at least eight characters, at least one lowercase character, one uppercase character, one number, and one special character. See the *vSphere Security* documentation for information about changing the password policy. The following characters are not supported in passwords: non-ASCII characters, semicolon (;), double quotation mark ("), single quotation mark ('), circumflex (^), and backslash (\).

7 Enter the site name for vCenter Single Sign-On.

The site name becomes important if you are using vCenter Single Sign-On in multiple locations. Choose your own name for the vCenter Single Sign-On site.

NOTE You cannot change the site name at a later time.

8 Review the installation options and click **Install.**

vCenter Single Sign-On is installed.

Install or Upgrade the vSphere Web Client

The vSphere Web Client lets you connect to a vCenter Server system to manage your vSphere deployment through a browser.

If an earlier version of the vSphere Web Client is installed, this procedure upgrades the vSphere Web Client.

NOTE vCenter Server 5.5 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPv4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

Prerequisites

- Download the vCenter Server installer. See "Download the vCenter Server Installer," on page 59.
- Verify that the system has an Internet connection.
- Verify that the system meets the software requirements for the vSphere Web Client. See "vSphere Web Client Software Requirements," on page 22.
- Before you install or upgrade any vSphere product, synchronize the clocks of all machines on the vSphere network. See "Synchronizing Clocks on the vSphere Network," on page 53.
- Install vCenter Single Sign-On, or upgrade to the current version.
- Verify that the vSphere Web Client and vCenter Server are registered to the same vCenter Single Sign-On server, to ensure that the vSphere Web Client can access the vCenter Server inventory.
- Close all browsers before installing or uninstalling the vSphere Web Client.
- Log in as a member of the Administrators group on the host machine, with a user name that does not contain any non-ASCII characters.

Procedure

1 In the software installer directory, double-click the `autorun.exe` file to start the installer.

2 Select **vSphere Web Client** and click **Install**.

3 Follow the prompts in the installation wizard to choose the installer language, and agree to the end user patent and license agreements.

4 Either accept the default destination folder or click **Change** to select another location.

The installation path cannot contain any of the following characters: non-ASCII characters, commas (,), periods (.), exclamation points (!), pound signs (#), at signs (@), or percentage signs (%).

If 8.3 name creation is disabled on the host machine, do not install the vSphere Web Clientin a directory that does not have an 8.3 short name or has a name that contains spaces. This situation will make the vSphere Web Client inaccessible.

5 Accept or change the default port settings.

6 Enter the information to register the vSphere Web Client with vCenter Single Sign-On.

The vCenter Single Sign-On administrator user name is administrator@vsphere.local, and the password must match the password you entered for the administrator user when you installed vCenter Single Sign-On. The Lookup Service URL takes the form https://*SSO_host_FQDN_or_IP*:7444/lookupservice/sdk, where 7444 is the default vCenter Single Sign-On HTTPS port number. Your entry should match the entry you made when you installed vCenter Single Sign-On. If you entered a different port number when you installed vCenter Single Sign-On, use that port number.

7 Click **Install**.

8 Start the vSphere Web Client by taking one of the following actions.

- If you are starting the vSphere Web Client for the first time, open a supported browser, and go to https://*vSphere_Web_Client_host_name_or_IP*:9443/vsphere-client.
- In subsequent sessions, you can start the vSphere Web Client from the Windows Start menu, by selecting **Programs > VMware > VMware vSphere Web Client > vSphere Web Client**.

NOTE After you upgrade the vSphere Web Client, when you log in for the first time, you may see the error message `Failed to navigate to desired location`. This can happen when a vSphere Web Client session from the previous version remains open when you upgrade. In this case, refresh the browser and log in again.

Migrate vSphere Web Client Data from a Windows Server 2003 Host

When you migrate from a Windows Server 2003 host to a host that is supported for the version 5.5 vCenter Server, you can also migrate some configuration data.

From your existing vSphere Web Client installation, migrate the data to the new host machine.

NOTE The file paths in this procedure assume that you install the vSphere Web Client

in the default location. If you use a different location, adjust the paths accordingly.

Prerequisites

- Verify that the new host machine meets the requirements for the version 5.5 vSphere Web Client. See Chapter 2, "System Requirements," on page 13.
- Review the topics in Chapter 3, "Preparing for the Upgrade to vCenter Server," on page 31
- In the existing vSphere Web Client host machine, verify that the VMware vSphere Web Client service is stopped, in the Windows Administrative Tools control panel, under Services.

Procedure

1 Copy the contents of the `SerenityDB` folder to the new host, at `C:\ProgramData\VMware\vSphere Web Client\SerenityDB`.

For version 5.0.x installations, the folder is located at `C:\Program Files\VMware\Infrastructure\vSphere Web Client\DMServer\SerenityDB`.

For version 5.1.x installations, the folder is located at `C:\Documents and Settings\All Users\Application Data\VMware\vSphere Web Client\SerenityDB`.

2 If you are migrating from the version 5.1.x vSphere Web Client, copy the `C:\Documents and Settings\All Users\Application Data\VMware\vSphere Web Client\webclient.properties` file to the new host, at `C:\ProgramData\VMware\vSphere Web Client\webclient.properties`.

The `webclient.properties` file does not exist in vSphere versions before 5.1.

3 Copy the vSphere Web Client `ssl` folder to the new host, at `C:\ProgramData\VMware\vSphere Web Client\ssl`.

   For version 5.0.x installations, the folder is located at `C:\Program Files\VMware\Infrastructure\vSphere Web Client\DMServer\config\ssl`.

   For version 5.1.x installations, the folder is located at `C:\Documents and Settings\All Users\Application Data\VMware\vSphere Web Client\ssl`.

4 Copy the vSphere Web Client `logs` folder to the new host, at `C:\ProgramData\VMware\vSphere Web Client\serviceability\logs`.

   For version 5.0.x installations, the folder is located at `C:\Program Files\VMware\Infrastructure\vSphere Web Client\DMServer\serviceability\logs`.

   For version 5.1.x installations, the folder is located at `C:\Documents and Settings\All Users\Application Data\VMware\vSphere Web Client\Logs`.

5 Copy the vSphere Web Client `eventlogs` folder to the new host, at `C:\ProgramData\VMware\vSphere Web Client\serviceability\eventlogs`.

   For version 5.0.x installations, the folder is located at `C:\Program Files\VMware\Infrastructure\vSphere Web Client\DMServer\serviceability\eventlogs`.

   For version 5.1.x installations, the folder is located at `C:\Documents and Settings\All Users\Application Data\VMware\vSphere Web Client\serviceability\eventlogs`.

Migrate vCenter Inventory Service Data from a Windows Server 2003 Host

When you migrate from a Windows Server 2003 host to a host that is supported for vCenter Single Sign-On 5.5, you can also migrate Inventory Service SSL certificates and configuration data.

NOTE The steps in this task assume that you install vCenter Server and components in the default location. If you use a different location, adjust the paths accordingly.

Prerequisites

- Verify that the host machine meets the requirements for vCenter Server 5.5. See Chapter 2, "System Requirements," on page 13.
- Review the topics in Chapter 3, "Preparing for the Upgrade to vCenter Server," on page 31.

Procedure

1 If the VMware vCenter Inventory Service is running, stop it.

   a From the Windows Start menu, select **Windows Administrative Tools > Services**.

   b Right-click **VMware vCenter Inventory Service** and click **Stop**.

2 Copy the SSL certificates from the `Inventory Service\ssl` folder of the source machine.

   For version 5.0.x installations, the folder is located at `C:\Program Files\VMware\Infrastructure\Inventory Service\ssl`.

   For version 5.1.x installations, the folder is located at `C:\Documents and Settings\All Users\Application Data\VMware\Infrastructure\Inventory Service\ssl`.

3 Create the following SSL folder on the host machine where you will install the new instance of Inventory Service: `C:\ProgramData\VMware\Infrastructure\Inventory Service\ssl`.

4 Paste the copied certificates in the folder `C:\ProgramData\VMware\Infrastructure\Inventory Service\ssl`.

5 Copy all data files from the `Inventory Service\data`folder

   For version 5.0.x installations, the folder is located at `C:\Program Files\VMware\Infrastructure\Inventory Service\data`.

   For version 5.1.x installations, the folder is located at `C:\Documents and Settings\All Users\Application Data\VMware\Infrastructure\Inventory Service\data`.

6 Create the following data folder on the host machine where you will install the new instance of Inventory Service: `C:\Program Files\VMware\Infrastructure\Inventory Service\data`.

7 Paste the copied data files in the folder `C:\Program Files\VMware\Infrastructure\Inventory Service\data`.

Install Inventory Service in a vCenter Server Migration from a Windows Server 2003 Host

After you migrate Inventory Service SSL certificates and configuration data from a Windows Server 2003 host to a host that is supported for Inventory Service 5.5, you can install Inventory Service on the new host.

NOTE vCenter Server 5.5 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPv4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

Prerequisites

- Verify that the new host machine meets the requirements for the version 5.5 vCenter Inventory Service. See Chapter 2, "System Requirements," on page 13.
- Review the topics in Chapter 3, "Preparing for the Upgrade to vCenter Server," on page 31.

Procedure

1 In the software installer directory, double-click the `autorun.exe` file to start the installer.

2 Select **vCenter Inventory Service** and click **Install.**

3 Follow the prompts in the installation wizard to choose the installer language, and agree to the end user patent and license agreements.

4 Accept or change the default installation folder.

   The installation path cannot contain any of the following characters: non-ASCII characters, commas (,), periods (.), exclamation points (!), pound signs (#), at signs (@), or percentage signs (%).

5 Enter the fully qualified domain name for the Inventory Service host machine.

6 Choose whether to keep the existing database or replace it with a new empty database.

7 Accept or change the default values for Inventory Service port numbers.

8 Select the size of your vCenter Server inventory to allocate memory for several Java services that are used by vCenter Server.

   This setting determines the maximum JVM heap settings for VMware VirtualCenter Management Webservices (Tomcat), Inventory Service, and Profile-Driven Storage Service. You can adjust this setting after installation if the number of hosts in your environment changes. See the recommendations in the topic vCenter Server Hardware Requirements.

9 Enter the information to register Inventory Service with vCenter Single Sign-On.

The vCenter Single Sign-On administrator user name is administrator@vsphere.local, and the password must match the password you entered when you installed vCenter Single Sign-On. The Lookup Service URL takes the form https://*SSO_host_FQDN_or_IP*:7444/lookupservice/sdk, where 7444 is the default vCenter Single Sign-On HTTPS port number. Your entry should match the entry you made when you installed vCenter Single Sign-On. If you entered a different port number when you installed vCenter Single Sign-On, use that port number.

NOTE If you installed vCenter Single Sign-On in a vCenter Server Appliance, you can enter the vCenter Single Sign-On administrator user as root@localos. In this case, the password is the root password of the vCenter Server Appliance. The Lookup Service URL takes the form https://*vCenter_Appliance_IP_or_host_name*:{7444}/lookupservice/sdk.

10 Click **Install Certificates**.

11 Click **Install**.

Inventory Service is installed with the SSL certificates and configuration data that you migrated from the Windows Server 2003 installation.

Migrate vCenter Server Data from a Windows Server 2003 Host

When you migrate from a Windows Server 2003 host to a host that is supported for vCenter Single Sign-On 5.5, you can also migrate the vCenter Server database and SSL certificates.

NOTE This task assumes that your existing vCenter Server uses a custom database. The steps in this task assume that you install vCenter Server and components in the default location. If you use a different location, adjust the paths accordingly.

Prerequisites

- Verify that the host machine meets the requirements for vCenter Server 5.5. See Chapter 2, "System Requirements," on page 13.
- Review the topics in Chapter 3, "Preparing for the Upgrade to vCenter Server," on page 31.

Procedure

1 If the VMware VirtualCenter Server service on the source host is running, stop it.

a In the Windows Administrative Tools control panel, double-click **Services**.

b Right-click **VMware VirtualCenter Server** and select **Stop**.

2 Copy the SSL certificates from the `VMware VirtualCenter\SSL` folder of the source machine.

The folder is located at `C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\SSL`.

3 Create the following SSL folder on the host machine where you will install the new instance of vCenter Server: `C:\ProgramData\VMware\VMwareVirtualCenter\SSL`.

4 Paste the copied certificates in the folder `C:\ProgramData\VMware\VMware VirtualCenter\SSL`.

5 Create a 64-bit DSN that points to the legacy vCenter Server database and database user.

Install vCenter Server in a Migration from a Windows Server 2003 Host

After you migrate vCenter Server SSL certificates from a Windows Server 2003 host to a host that is supported for vCenter Server 5.5, you can install vCenter Server on the new host.

If you do not enter a license key, vCenter Server will be in evaluation mode, which allows you to use the full feature set for a 60-day evaluation period. After installation, you can enter the license key to convert vCenter Server to licensed mode.

NOTE vCenter Server 5.5 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPv4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

Prerequisites

- Verify that the new host machine meets the requirements for the version 5.5 vCenter Inventory Service. See Chapter 2, "System Requirements," on page 13.
- Review the topics in Chapter 3, "Preparing for the Upgrade to vCenter Server," on page 31.
- To install the vCenter Server on a drive other than `C:`, verify that there is enough space in the `C:` drive to install the Microsoft Windows Installer `.msi` file.

Procedure

1. In the software installer directory, double-click the `autorun.exe` file to start the installer.
2. Select **vCenter Server** and click **Install**.
3. Follow the prompts in the installation wizard to choose the installer language, and agree to the end user patent and license agreements.
4. Click **Use an existing supported database** and select your legacy database from the list of available DSNs. Enter the user name and password for the DSN.

   NOTE You might get a warning that the DSN points to an older version of a repository that must be upgraded. If you click **Yes**, the installer upgrades the database schema, making the database irreversibly incompatible with previous VirtualCenter versions.

5. If the installer prompts you, enter the JDBC URL for your existing vCenter Server database.

   The installer should generate and validate the JDBC URL for the vCenter Server database. If the installer fails to connect to the database by using the generated JDBC URL, the installer prompts you to specify the JDBC URL.

6. If the installer warns that the DSN points to an older version of a repository that must be upgraded, click **Yes**.

   The installer upgrades the database schema, making the database irreversibly incompatible with previous vCenter Server versions.

7. Enter the administrator name and password that you use when you log in to the system on which you are installing vCenter Server.

   You need the user name and password to log in to vCenter Server after you install it.

   The Fully Qualified Domain Name text box displays the FQDN of the system that you are installing vCenter Server on. The vCenter Server installer checks that the FQDN is resolvable. If not, a warning message appears when you click **Next**. Change the entry to a resolvable FQDN. You must enter the FQDN, not the IP address.

8 Select **Create a standalone VMware vCenter Server instance** or **Join a VMware vCenter Group using Linked Mode to share information**.

Joining a Linked Mode group enables the vSphere Web Client to view, search, and manage data across multiple vCenter Server systems.

NOTE This option does not appear if you are upgrading the VirtualCenter or vCenter Server database schema. You can join a Linked Mode group after the installation is complete.

9 If you join a group, enter the fully qualified domain name and LDAP port number of any remote vCenter Server system.

10 Accept or change the port numbers to connect to vCenter Server.

11 (Optional) Select **Increase the number of available ephemeral ports**.

12 Select the size of your vCenter Server inventory to allocate memory for several Java services that are used by vCenter Server.

This setting determines the maximum JVM heap settings for VMware VirtualCenter Management Webservices (Tomcat), Inventory Service, and Profile-Driven Storage Service. You can adjust this setting after installation if the number of hosts in your environment changes. See the recommendations in the topic vCenter Server Hardware Requirements.

13 Enter the information to register vCenter Server with vCenter Single Sign-On.

The vCenter Single Sign-On administrator user name is administrator@vsphere.local, and the password must match the password you entered when you installed vCenter Single Sign-On. The Lookup Service URL takes the form https://*SSO_host_FQDN_or_IP*:7444/lookupservice/sdk, where 7444 is the default vCenter Single Sign-On HTTPS port number. Your entry should match the entry you made when you installed vCenter Single Sign-On. If you entered a different port number when you installed vCenter Single Sign-On, use that port number.

NOTE If you installed vCenter Single Sign-On in a vCenter Server Appliance, you can enter the vCenter Single Sign-On administrator user as root@localos. In this case, the password is the root password of the vCenter Server Appliance. The Lookup Service URL takes the form https://*vCenter_Appliance_IP_or_host_name*:{7444}/lookupservice/sdk.

14 If prompted to install or overwrite a certificate, follow the prompt.

15 Register a vCenter Server administrator with vCenter Single Sign-On, and select the check box if the administrator is a group.

The administrator or group you register here is granted the necessary privileges to administer the vCenter Server instance that you are installing.

16 Enter the Inventory Service URL.

The Inventory Service URL takes the form https://*Inventory_Service_host_FQDN_or_IP*:10443. 10443 is the default Inventory Service HTTPS port number. If you entered a different port number when you installed Inventory Service, use that port number here.

17 Either accept the default destination folder or click **Change** to select another location.

The installation path cannot contain any of the following characters: non-ASCII characters, commas (,), periods (.), exclamation points (!), pound signs (#), at signs (@), or percentage signs (%).

18 Click **Install**.

Multiple progress bars appear during the installation of the selected components.

19 Click **Finish**.

vCenter Server is installed with the migrated SSL certifiicates and vCenter Server database from your Windows Server 2003 installation.

What to do next

After you complete the installation, use the vSphere Web Client to connect to vCenter Server.

Review the topics in Chapter 5, "After You Upgrade vCenter Server," on page 127 for other postinstallation actions you might want to take.

vCenter Single Sign-On Installation Fails

In a Windows environment, vCenter Single Sign-On installation might fail for several reasons.

Problem

The vCenter Single Sign-On installation fails in a Windows environment.

Cause

Multiple causes of an installation failure.

Solution

1 Verify that all installation setup prerequisites are met.

   At the time the installation fails, the installer displays a message similar to `####: Installation failed due to....`

2 At a command line, run the following command to gather a vCenter Single Sign-On support bundle.

   ```
   C:\Windows\System32\cscript.exe "SSO Server\scripts\sso-support.wsf" /z
   ```

3 Click **OK**

4 View the logs in `%TEMP%\vminst.log` for details about the failure and possible solutions.

   For a complete list of logs, see VMware Knowledge Base article 2033430.

Updating vCenter Server with Service Packs

VMware provides service packs to update the vCenter Server 5.x software and third-party components.

vCenter Server service pack releases can include updates to vCenter Server, Inventory Service, vCenter Single Sign On, and Profile-Driven Storage Service.

vCenter Server 5.x service packs will be available from the VMware Web site. The service pack update process updates files and registry settings required by vCenter Server, and restart Windows services that are stopped during the update.

NOTE Installing an update on Windows Server 2008 or later with User Account Control (UAC) turned on requires Administrator privileges. The logged in user must be Administrator, or an Administrators group member whose privileges are elevated to the Administrator level. See "Elevate Administrators Group Privileges to Administrator Level in Windows Server 2008," on page 119.

Elevate Administrators Group Privileges to Administrator Level in Windows Server 2008

Installing a vCenter Server update on Windows Server 2008 or later with User Account Control (UAC) turned on requires the logged in user to have Administrator-level privileges. You can elevate the privileges of Administrators group members to the Administrator level.

Alternatively, you can turn off UAC in the User Accounts control panel, and turn it back on after the update is complete.

Procedure

1 In the Administrative Tools control panel, double-click **Local Security Policy**.

2 Under Local Policies, select **Security Options**.

3 Double-click **User Account Control: Run all administrators in Admin Approval Mode**.

4 Select **Disabled** and click **OK.**

All members of the Administrators group can install the update.

What to do next

After you install the update, you can reenable User Account Control: Run all administrators in Admin Approval Mode.

Upgrading and Updating the vCenter Server Appliance

You can upgrade the vCenter Server Appliance by deploying a new version of the appliance. You can update the vCenter Server Appliance from a VMware.com repository, a zipped update bundle, or the CD-ROM drive.

Upgrade the VMware vCenter Server Appliance

For upgrades to the vCenter Server Appliance, you can deploy a new version of the appliance and import the network identity of your existing vCenter Server Appliance.

NOTE The upgrade from version 5.0 to 5.5 differs slightly from the upgrade from version 5.1 to 5.5. Options for setting roles are not available during the upgrade from version 5.1 to 5.5.

VMware product versions are numbered with two digits, for example, vSphere 5.5. A release that changes either digit, for example, from 4.1 to 5.0, or from 5.1 to 5.5, involves major changes in the software, and requires an upgrade from the previous version. A release that makes a smaller change, requiring only an update, is indicated by an update number, for example, vSphere 5.1 Update 1.

For updates to the vCenter Server Appliance, for example, from version 5.1 to version 5.1 Update 1, see "Update the VMware vCenter Server Appliance from a VMware.com Repository," on page 122, "Update the VMware vCenter Server Appliance from a Zipped Update Bundle," on page 122, and "Update the VMware vCenter Server Appliance from the CD-ROM Drive," on page 123.

Versions 5.0 Update 1 and later, 5.1.x, and 5.5 of the vCenter Server Appliance use PostgreSQL for the embedded database instead of IBM DB2, which was used in vCenter Server Appliance 5.0. If you use the embedded database with the vCenter Server Appliance, when you upgrade from version 5.0 to version 5.5, the embedded IBM DB2 database is migrated to a PostgreSQL database. The configuration state of your existing database is preserved and the schema is upgraded to be compatible with vCenter Server Appliance 5.5.

NOTE vCenter Server 5.5 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPv4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

Version 5.5 of the vCenter Server Appliance is deployed with virtual hardware version 7, which supports eight virtual CPUs per virtual machine in ESXi. Depending on the hosts that you will manage with the vCenter Server Appliance, you might want to upgrade the ESXi hosts and update the hardware version of the vCenter Server Appliance to support more virtual CPUs:

- ESXi 4.x supports up to virtual hardware version 7 with up to 8 virtual CPUs per virtual machine.
- ESXi 5.0.x supports up to virtual hardware version 8 with up to 32 virtual CPUs per virtual machine.
- ESXi 5.1.x supports up to virtual hardware version 9 with up to 64 virtual CPUs per virtual machine.

CAUTION If you update the vCenter Server appliance to hardware version 10, you cannot edit the virtual machine settings for the appliance using the vSphere Client. This might cause difficulties in managing the vCenter Server Appliance, because you cannot use the vSphere Web Client to connect directly to the host on which the vCenter Server Appliance resides to manage it. Do not upgrade the vCenter Server Appliance to hardware version 10.

To update the virtual hardware version of a virtual machine, see the information about virtual machine compatibility levels in the *vSphere Virtual Machine Administration* documentation.

NOTE If your upgrade reconfigures the appliance to use an external vCenter Single Sign-On instance on a Microsoft Windows host, after the upgrade, you cannot log in as `root` unless you add a user by that name to the vCenter Single Sign-On host. Windows does not include a `root` user by default.

Prerequisites

- Verify that the clocks of all machines on the vSphere network are synchronized. See "Synchronizing Clocks on the vSphere Network," on page 53.
- If your vCenter Server Appliance uses an external instance of vCenter Single Sign-On, upgrade Single Sign-On to the same version as the vCenter Server Appliance version that you are upgrading to.
- Verify that the vCenter Server SSL certificate for your existing vCenter Server Appliance is configured correctly. See VMware Knowledge Base article 2057223.
- Back up the vCenter Server database.
- Create a snapshot of the vCenter Server Appliance.

Procedure

1 Deploy the new version of the vCenter Server Appliance.

  The new appliance has a default network configuration, and the vCenter Server service is unconfigured and disabled. You do not need to configure NFS on the new appliance. This configuration is copied automatically on upgrade.

2 Make sure that the new appliance has at least the same amount of RAM and number of CPUs as the old appliance.

3 If you added additional disks or increased the size of the VMDKs of the old appliance, reconfigure the new appliance to have at least the same disk space as the old appliance.

4 Connect to both the old and new appliances in separate browser windows.

5 In the new appliance, in the vCenter Server Setup wizard, accept the end user license agreement.

The wizard is started automatically on first login. On subsequent logins, you can start the wizard manually, by clicking the **Launch** button in the Utilities section of the startup page.

6 In the new appliance, in the Configure Options panel, select **Upgrade from previous version**.

7 In the new appliance, click **Next**.

8 If you are upgrading from version 5.0.x: in the old appliance, in the **Upgrade** tab, select **source** for the appliance role, and click **Set role**.

9 In the new appliance, copy the local appliance key.

10 Import the key that you copied in the previous step into the old appliance.

- If you are upgrading from version 5.0.x: in the old appliance, go to the **Upgrade** tab, **Establish Trust** subtab. Paste the key into the **Remote Appliance Key** field and click **Import remote key**.
- If you are upgrading from version 5.1.x: in the old appliance, paste the key into the **Upgrade key** box, and click **Import key and stop vCenter Server**.

11 In the old appliance, copy the local appliance key.

12 In the new appliance, paste the key that you copied in the previous step into the **Upgrade key** box and click **Next**.

The setup performs a check on the SSL certificate of the old appliance. If problems are found, the Setup wizard displays a panel that explains the problem and provides an option to generate a new self-signed certificate for the new appliance.

13 If you want to keep the current certificate and manually correct any resulting problems, uncheck the checkbox **Replace the vCenter SSL certificate**.

If you are upgrading from a version 5.1.x appliance, the existing Single Sign-On configuration will be used for the upgraded appliance. Proceed to Step 15. If you are upgrading from a version 5.0 appliance, the wizard displays the SSO Settings panel.

14 If you are upgrading from a version 5.0 appliance, in the SSO settings panel, choose whether to use an external instance of Single Sign-On, or the embedded version.

If you choose an external Single Sign-On instance, a check is performed to ensure that the external Single Sign-On version is 5.5. If the version is earlier than 5.5, an error message is displayed and the upgrade will not proceed.

15 In the new appliance, click **Next**.

16 Review the list of hosts managed by the source appliance and select the hosts on which to run pre-upgrade checks.

To minimize the chance of problems with the upgrade, run the pre-upgrade checks on all hosts, or at least on the most important hosts.

17 Review the pre-upgrade check of the source appliance hosts and correct any errors before proceeding.

18 Confirm that you have taken a backup or snapshot of the source appliance and external database, and click **Next**.

The new appliance shuts down the old appliance and assumes the network identity of the old appliance. If the old appliance was configured to use dynamic addressing, the new appliance will also use dynamic addressing. When the import is complete, the new vCenter Server Appliance starts.

19 When the upgrade is complete, click **Close**.

The vCenter Server Appliance is upgraded and the new appliance will reboot.

Update the VMware vCenter Server Appliance from a VMware.com Repository

You can set the vCenter Server Appliance to update itself automatically from a public repository on the VMware.com Web site when VMware releases a new update.

To update the vCenter Server Appliance from a zipped update bundle that you download to your own internal repository, see "Update the VMware vCenter Server Appliance from a Zipped Update Bundle," on page 122. To update the vCenter Server Appliance from the virtual CD-ROM drive of the appliance, see "Update the VMware vCenter Server Appliance from the CD-ROM Drive," on page 123. For major upgrades to the vCenter Server Appliance, see "Upgrade the VMware vCenter Server Appliance," on page 119.

Prerequisites

- Verify that the clocks of all machines on the vSphere network are synchronized. See "Synchronizing Clocks on the vSphere Network," on page 53.
- Back up the vCenter Server database.

Procedure

1 Open the management vCenter Virtual Appliance Web interface on port 5480.

2 In the **Update** tab, click **Settings**.

3 (Optional) Under **Automatic Updates**, set and schedule the vCenter Server Appliance to check for and install updates.

4 Under **Update Repository**, select **Use Default Repository**.

The default repository is set to the correct VMware.com URL.

5 Click **Save Settings**.

6 Click **Status**.

7 Under **Actions**, click **Check Updates** or **Install Updates**.

Update the VMware vCenter Server Appliance from a Zipped Update Bundle

If your Internet access is restricted, you can set up your own internal repository for updates, instead of getting updates from a VMware public repository. You can download updates as a zipped update bundle.

To update the vCenter Server Appliance from a VMware public repository, see "Update the VMware vCenter Server Appliance from a VMware.com Repository," on page 122. To update the vCenter Server Appliance from the virtual CD-ROM drive of the appliance, see "Update the VMware vCenter Server Appliance from the CD-ROM Drive," on page 123. For major upgrades to the vCenter Server Appliance, see "Upgrade the VMware vCenter Server Appliance," on page 119.

Prerequisites

- Verify that the clocks of all machines on the vSphere network are synchronized. See "Synchronizing Clocks on the vSphere Network," on page 53.

- Back up the vCenter Server database.

Procedure

1. Download the zipped updated bundle from the VMware.com Web site.
2. On your chosen Web server, create a repository directory under the root: for example, `vc_update_repo`.
3. Extract the zipped bundle into the repository directory.

   The extracted files are in two subdirectories: `manifest` and `package-pool`.
4. Open the management vCenter Virtual Appliance Web interface on port 5480.
5. In the **Update** tab, click **Settings**.
6. Select **Use Specified Repository**.
7. For the Repository URL, enter the URL of the repository you created.

   For example, if the repository directory is `vc_update_repo`, the URL should be similar to the following URL: `http://web_server_name.your_company.com/vc_update_repo`
8. Click **Save Settings**.
9. Click **Status**.
10. Under **Actions**, click **Install Updates**.

The update is installed.

Update the VMware vCenter Server Appliance from the CD-ROM Drive

You can update the vCenter Server Appliance from an ISO file that the appliance reads from the virtual CD-ROM drive.

To update the vCenter Server Appliance from a zipped update bundle that you download to your own internal repository, see "Update the VMware vCenter Server Appliance from a Zipped Update Bundle," on page 122. To update the vCenter Server Appliance from a VMware public repository, see "Update the VMware vCenter Server Appliance from a VMware.com Repository," on page 122. For major upgrades to the vCenter Server Appliance, see "Upgrade the VMware vCenter Server Appliance," on page 119.

Prerequisites

- Verify that the clocks of all machines on the vSphere network are synchronized. See "Synchronizing Clocks on the vSphere Network," on page 53.
- Back up the vCenter Server database.

Procedure

1. Download the update ISO file from the VMware.com Web site.
2. Connect the vCenter Server Appliance CD-ROM drive to the ISO file you downloaded.
3. Open the management vCenter Virtual Appliance Web interface on port 5480.
4. In the **Update** tab, click **Settings**.
5. Under **Update Repository**, select **Use CD-ROM Updates**.
6. Click **Save Settings**.
7. Click **Status**.
8. Under **Actions**, click **Install Updates**.

Install or Upgrade vCenter Server Java Components Separately

The required vCenter Server Java Components (JRE) are installed or upgraded silently when you install or upgrade vCenter Server. You can also install or upgrade vCenter Server Java Components separately.

By using the separate installer, you can update or upgrade JRE to a version that is released asynchronously from vCenter Server releases. If an earlier version of JRE is present on the system, this procedure upgrades the existing JRE version.

Prerequisites

- Verify that Microsoft Windows Installer 3.0 or later is present on your system.
- Download the vCenter Server installer from the VMware downloads page at http://www.vmware.com/support/ and extract the zip archive.

Procedure

1. In Windows Explorer, double-click the file *vCenter_Server_installation_directory*`/vJRE/VMware-jre.exe`.

   The VMware vCenter Server - Java Components installer wizard opens.
2. Accept the license agreement.
3. Accept or change the default installation folder.
4. Click **Install.**

The vCenter Server Java Components (JRE) are installed or upgraded.

Install or Upgrade vCenter Server tc Server Separately

The required vCenter Server component tc Server is installed or upgraded silently when you install or upgrade vCenter Server. You can also install or upgrade vCenter Server tc Server separately.

By using the separate installer, you can update or upgrade vCenter Server tc Server to a version that is released asynchronously from vCenter Server releases. If an earlier version of vCenter Server tc Server is present on the system, this procedure upgrades the existing vCenter Server tc Server version.

Prerequisites

- Verify that Microsoft Windows Installer 3.0 or later is present on your system.
- Download the vCenter Server installer from the VMware downloads page at http://www.vmware.com/support/ and extract the zip archive.

Procedure

1. In Windows Explorer, double-click the file *vCenter_Server_installation_directory*`/vtcServer/VMware-tcserver.exe`.

   The VMware vCenter Server - tc Server installer wizard opens.
2. Accept the license agreement.
3. Accept or change the default installation folder.
4. Click **Install.**

vCenter Server tc Server is installed or upgraded.

Update the Java Components and vCenter Server tc Server with VIMPatch

You can separately update the Java version of all vCenter Server components depending on JRE server by using the `VIMPatch` ISO file. You can also upgrade the vCenter Server tc Server by using the same patch.

The following vCenter Server components depend on Java:

- vCenter Single Sign-On
- vCenter Inventory Service
- vCenter Server
- vSphere Web Client
- vCenter Orchestrator

You can apply the patch without reinstalling the vCenter Server components. The patch delivers updates for JRE and vCenter Server tc Server.

If vCenter Server tc Server is present on the system, where the respective vCenter Server component is installed, this procedure also upgrades vCenter Server tc Server version.

Prerequisites

- Download the Java Components patch from VMware downloads page at https://my.vmware.com/web/vmware/downloads. The name format is `VMware-VIMPatch-5.5.0-`*`build_number-YYYYMMDD`*`.iso`.
- Stop any vCenter Server component operations, as when you apply the patch, all running services will be stopped.

Procedure

1. Mount the `VMware-VIMPatch-5.5.0-`*`build_number-YYYYMMDD`*`.iso` to the system where the vCenter Server component is installed.
2. Double-click *`ISO_mount_directory`*`/autorun.exe`.

   A vCenter Server Java Components Update wizard opens.
3. Click **Patch All**.

   The patch checks whether the Java components are up to date, and silently upgrades them if necessary.

   If vCenter Server tc Server is present on the system, it is also upgraded.

vCenter Server Upgrade Fails When Unable to Stop Tomcat Service

A vCenter Server upgrade can fail when the installer is unable to stop the Tomcat service.

Problem

If the vCenter Server installer cannot stop the Tomcat service during an upgrade, the upgrade fails with an error message similar to `Unable to delete VC Tomcat service`. This problem can occur even if you stop the Tomcat service manually before the upgrade, if some files that are used by the Tomcat process are locked.

Solution

1. From the Windows **Start** menu, select **Settings > Control Panel > Administrative Tools > Services**.
2. Right-click **VMware VirtualCenter Server** and select **Manual**.
3. Right-click **VMware vCenter Management Webservices** and select **Manual**.

4 Reboot the vCenter Server machine before upgrading.

   This releases any locked files that are used by the Tomcat process, and enables the vCenter Server installer to stop the Tomcat service for the upgrade.

Alternatively, you can restart the vCenter Server machine and restart the upgrade process, but select the option not to overwrite the vCenter Server data.

After You Upgrade vCenter Server 5

After you upgrade to vCenter Server, consider the postupgrade options and requirements.

- To view the database upgrade log, open `%TEMP%\VCDatabaseUpgrade.log`.
- Upgrade any additional modules that are linked to this instance of vCenter Server, such as vSphere Update Manager.
- On the VMware Web site, log in to your account page to access the license portal. From the license portal, upgrade your vCenter Server license. Using the vSphere Web Client, assign the upgraded license key to the vCenter Server host.
- For Oracle databases, copy the Oracle JDBC Driver (`ojdbc14.jar` or `ojdbc5.jar`) to the`[VMware vCenter Server]\tomcat\lib` folder.
- For SQL Server databases, if you enabled bulk logging for the upgrade, disable it after the upgrade is complete.
- Optionally, join the vCenter Server system to a Linked Mode group.
- Optionally, upgrade or migrate the ESXi or ESX hosts in the vCenter Server inventory to the same version you upgraded vCenter Server to.
- If it is not enabled, enable SSL certification checking for all vSphere HA clusters. SSL certification checking is required to configure HA on the hosts. In vCenter Server, select **Administration > vCenter Server Settings > SSL Settings > vCenter requires verified host SSL certificates**. Follow the instructions to verify each host SSL certificate and click **OK**. If necessary, reconfigure HA on the hosts.

This chapter includes the following topics:

Install or Upgrade the vSphere Web Client

The vSphere Web Client lets you connect to a vCenter Server system to manage your vSphere deployment through a browser.

If an earlier version of the vSphere Web Client is installed, this procedure upgrades the vSphere Web Client.

NOTE vCenter Server 5.5 supports connection between vCenter Server and vCenter Server components by IP address only if the IP address is IPv4-compliant. To connect to a vCenter Server system in an IPv6 environment, you must use the fully qualified domain name (FQDN) or host name of the vCenter Server. The best practice is to use the FQDN, which works in all cases, instead of the IP address, which can change if assigned by DHCP.

Prerequisites

- Download the vCenter Server installer. See "Download the vCenter Server Installer," on page 59.
- Verify that the system has an Internet connection.
- Verify that the system meets the software requirements for the vSphere Web Client. See "vSphere Web Client Software Requirements," on page 22.
- Before you install or upgrade any vSphere product, synchronize the clocks of all machines on the vSphere network. See "Synchronizing Clocks on the vSphere Network," on page 53.
- Install vCenter Single Sign-On, or upgrade to the current version.
- Verify that the vSphere Web Client and vCenter Server are registered to the same vCenter Single Sign-On server, to ensure that the vSphere Web Client can access the vCenter Server inventory.
- Close all browsers before installing or uninstalling the vSphere Web Client.
- Log in as a member of the Administrators group on the host machine, with a user name that does not contain any non-ASCII characters.

Procedure

1. In the software installer directory, double-click the `autorun.exe` file to start the installer.
2. Select **vSphere Web Client** and click **Install**.
3. Follow the prompts in the installation wizard to choose the installer language, and agree to the end user patent and license agreements.
4. Either accept the default destination folder or click **Change** to select another location.

   The installation path cannot contain any of the following characters: non-ASCII characters, commas (,), periods (.), exclamation points (!), pound signs (#), at signs (@), or percentage signs (%).

   If 8.3 name creation is disabled on the host machine, do not install the vSphere Web Clientin a directory that does not have an 8.3 short name or has a name that contains spaces. This situation will make the vSphere Web Client inaccessible.
5. Accept or change the default port settings.
6. Enter the information to register the vSphere Web Client with vCenter Single Sign-On.

   The vCenter Single Sign-On administrator user name is administrator@vsphere.local, and the password must match the password you entered for the administrator user when you installed vCenter Single Sign-On. The Lookup Service URL takes the form https://*SSO_host_FQDN_or_IP*:7444/lookupservice/sdk, where 7444 is the default vCenter Single Sign-On HTTPS port number. Your entry should match the entry you made when you installed vCenter Single Sign-On. If you entered a different port number when you installed vCenter Single Sign-On, use that port number.

7 Click **Install**.

8 Start the vSphere Web Client by taking one of the following actions.

- If you are starting the vSphere Web Client for the first time, open a supported browser, and go to https://*vSphere_Web_Client_host_name_or_IP*:9443/vsphere-client.
- In subsequent sessions, you can start the vSphere Web Client from the Windows Start menu, by selecting **Programs > VMware > VMware vSphere Web Client > vSphere Web Client**.

NOTE After you upgrade the vSphere Web Client, when you log in for the first time, you may see the error message `Failed to navigate to desired location`. This can happen when a vSphere Web Client session from the previous version remains open when you upgrade. In this case, refresh the browser and log in again.

Install a Local Copy of vSphere Web Client Help

If you do not have internet access from the system you use to access the vSphere Web Client, you can download and deploy a local copy of the online Help.

By default, vSphere Web Client accesses online Help on the Web. This allows the client to access the most up-to-date version of the Help content.

If you download and deploy Help locally, the local copy is not updated when new Help is published to the Web. If you deploy local Help, check the download location periodically for updates.

For instructions for downloading and deploying vSphere Web Client online Help locally, see http://kb.vmware.com/kb/2030344.

Install or Upgrade vSphere ESXi Dump Collector

You can configure ESXi to dump the vmkernel memory to a network server, rather than to a disk, when the system has encountered a critical failure. Install vSphere ESXi Dump Collector to collect such memory dumps over the network.

If an earlier version of the vSphere ESXi Dump Collector is installed on your system, this procedure upgrades the vSphere ESXi Dump Collector to the current version.

NOTE In the vCenter Server Appliance, the vSphere ESXi Dump Collector is installed and enabled by default. These instructions apply to Windows-based deployments.

For instructions on configuring ESXi to dump kernel memory to the network server, see the information about configuring the vSphere ESXi Dump Collector with esxcli in the *vSphere Installation and Setup* documentation.

The vSphere ESXi Dump Collector is most useful for datacenters where ESXi hosts are configured using the Auto Deploy process, so the ESXi hosts might not have local storage. You can also install the vSphere ESXi Dump Collector for ESXi hosts that do have local storage, as an additional location where vmkernel memory dumps can be redirected when critical failures occur.

You can install the vSphere ESXi Dump Collector on the same machine as the associated vCenter Server, or on a different machine that has network connection to the vCenter Server.

The vSphere ESXi Dump Collector service binds to an IPv4 address for communication with vCenter Server, and does not support IPv6. The vCenter Server can be on a host machine in an IPv4-only, IPv4/IPv6 mixed-mode, or IPv6-only network environment, but the machine that connects to the vCenter Server through the vSphere Web Client must have an IPv4 address for the vSphere ESXi Dump Collector service to work.

Prerequisites

- Verify that you have administrator privileges

- Verify that the host machine has Windows Installer 3.0 or later.
- Verify that the host machine has a supported processor and operating system. The vSphere ESXi Dump Collector supports the same processors and operating systems as vCenter Server. See "vCenter Server Software Requirements," on page 22 and "Hardware Requirements for vCenter Server, the vSphere Web Client, vCenter Inventory Service, and vCenter Single Sign-On," on page 17.
- Verify that the host machine has a valid IPv4 address. You can install the vSphere ESXi Dump Collector on a machine in an IPv4-only or IPv4/IPv6 mixed-mode network environment, but you cannot install the vSphere ESXi Dump Collector on a machine in an IPv6-only environment.
- If you are using a network location for the Dump Collector repository, make sure the network location is mounted.

Gather the following information to complete the installation or upgrade:

- The location to install the vSphere ESXi Dump Collector to, if you are not using the default location.
- The location for the vSphere ESXi Dump Collector repository where the dump files will be stored.
- (Optional) The maximum size for the vSphere ESXi Dump Collector repository. The specified network location must have at least that much free space.
- Whether to install the vSphere ESXi Dump Collector as a standalone instance or to integrate the vSphere ESXi Dump Collector with a vCenter Server. The vSphere ESXi Dump Collector is not supported for integration with vCenter Server versions earlier than version 5.0.
- If the vSphere ESXi Dump Collector is integrated with a vCenter Server, the address and credentials for the vCenter Server: IP address or name, HTTP port, user name, and password.
- The vSphere ESXi Dump Collector server port, if you are not using the default setting.
- The host name or IP address to identify the vSphere ESXi Dump Collector on the network.
- The credentials of a user authorized to register or update the vSphere ESXi Dump Collector extension with vCenter Server.

Table 5-1. Extension Privileges

Privilege Name	Description
Extension.Register extension	Allows registration of an extension (plug-in).
Extension.Unregister extension	Allows unregistering an extension (plug-in).
Extension.Update extension	Allows updates to an extension (plug-in).

Procedure

1. In the software installer directory, double-click the `autorun.exe` file to start the installer.
2. Select **vSphere ESXi Dump Collector** and click **Install**.
3. Follow the wizard prompts to complete the installation or upgrade.

Install or Upgrade vSphere Syslog Collector

Install the vSphere Syslog Collector to enable ESXi system logs to be directed to a server on the network, rather than to a local disk.

If an earlier version of vSphere Syslog Collector is installed on your system, this procedure upgrades vSphere Syslog Collector to the current version.

You can install vSphere Syslog Collector on the same machine as the associated vCenter Server, or on a different machine that has network connection to the vCenter Server. The vSphere Syslog Collector service binds to an IPv4 address for communication with vCenter Server, and does not support IPv6. The vCenter Server can be on a host machine in an IPv4-only, IPv4/IPv6 mixed-mode, or IPv6-only network environment, but the machine that connects to the vCenter Server through the vSphere Web Client must have an IPv4 address for the vSphere Syslog Collector service to work.

Prerequisites

- Verify that you have administrator privileges.
- Verify that the host machine has Windows Installer 3.0 or later.
- Verify that the host machine has a supported processor and operating system. vSphere Syslog Collector supports the same processors and operating systems as vCenter Server. See "vCenter Server Software Requirements," on page 22 and "Hardware Requirements for vCenter Server, the vSphere Web Client, vCenter Inventory Service, and vCenter Single Sign-On," on page 17.
- Determine whether to install vSphere Syslog Collector as a standalone instance or to integrate vSphere Syslog Collector with a vCenter Server. vSphere Syslog Collector is not supported for integration with vCenter Server versions earlier than version 5.0.
- Verify that the host machine has a valid IPv4 address. You can install vSphere Syslog Collector on a machine in an IPv4-only or IPv4/IPv6 mixed-mode network environment, but you cannot install vSphere Syslog Collector on a machine in an IPv6-only environment.

Gather the following information to complete the installation or upgrade:

- The location to install vSphere Syslog Collector, if you are not using the default location.
- The location for the vSphere Syslog Collector repository where the syslog files will be stored.
- (Optional) The maximum size for the vSphere Syslog Collector repository. The specified network location must have at least that much free space.
- (Optional) The maximum number of vSphere Syslog Collector log rotations to keep.
- If vSphere Syslog Collector is integrated with a vCenter Server, the address and credentials for the vCenter Server: IP address or name, HTTP port, user name, and password.
- The vSphere Syslog Collector server port, if you are not using the default setting, and whether to use TCP and UDP protocols for this port.
- The vSphere Syslog Collector server SSL port, if you are not using the default setting, and whether to use secure connection (SSL) for this port.
- The host name or IP address to identify vSphere Syslog Collector on the network.

Procedure

1. In the software installer directory, double-click the `autorun.exe` file to start the installer.
2. Select **vSphere Syslog Collector** and click **Install**.
3. Follow the wizard prompts to complete the installation or upgrade.

Install or Upgrade vSphere Auto Deploy

Install vSphere Auto Deploy to provision and customize physical hosts by loading the ESXi image directly into memory. You can provision and reprovision hundreds of ESXi hosts efficiently with vCenter Server.

If an earlier version of vSphere Auto Deploy is installed on your system, this procedure upgrades vSphere Auto Deploy to the current version.

You must install the vSphere Auto Deploy server separately for each instance of vCenter Server that you plan to use the vSphere Auto Deploy with. vSphere Auto Deploy is not supported with vCenter Server versions earlier than version 5.0. You must upgrade vSphere Auto Deploy when you upgrade vCenter Server. vSphere Auto Deploy is supported only in the same version as the corresponding vCenter Server.

vSphere Auto Deploy supports both IPv4 and IPv6. However, vSphere Auto Deploy uses a PXE boot infrastructure that supports only IPv4. You can use vSphere Auto Deploy in a mixed IPv4-IPv6 environment or an IPv4-only environment, but not in an IPv6-only environment.

Prerequisites

- Verify that you have administrator privileges
- Verify that the host machine has Windows Installer 3.0 or later.
- Verify that the host machine has a supported processor and operating system. vSphere Auto Deploy supports the same processors and operating systems as vCenter Server.

Gather the following information to complete the installation or upgrade:

- The location to install vSphere Auto Deploy in, if you are not using the default location.
- The location for the vSphere Auto Deploy repository. Do not use a network share for the repository.
- (Optional) The maximum size for the vSphere Auto Deploy repository. Best practice is to allocate 2GB to have enough room for four image profiles and some extra space. Each image profile requires approximately 350MB. Determine how much space to reserve for the vSphere Auto Deploy repository by considering how many image profiles you expect to use. The specified disk must have at least that much free space.
- The address and credentials of the vCenter Server that you are installing the vSphere Auto Deploy feature for: IP address or name, HTTP port, user name, and password.
- The vSphere Auto Deploy server port, if you are not using the default setting.
- The host name or IP address to identify vSphere Auto Deploy on the network.

Procedure

1 In the software installer directory, double-click the `autorun.exe` file to start the installer.

2 Select **vSphere Auto Deploy** and click **Install**.

3 Follow the wizard prompts to complete the installation or upgrade.

Install or Upgrade vSphere Authentication Proxy

Install vSphere Authentication Proxy to enable ESXi hosts to join a domain without using Active Directory credentials. vSphere Authentication Proxy enhances security for PXE-booted hosts and hosts that are provisioned using Auto Deploy, by removing the need to store Active Directory credentials in the host configuration.

If an earlier version of the vSphere Authentication Proxy is installed on your system, this procedure upgrades the vSphere Authentication Proxy to the current version.

You can install vSphere Authentication Proxy on the same machine as the associated vCenter Server, or on a different machine that has network connection to the vCenter Server. The vSphere Authentication Proxy is not supported with vCenter Server versions earlier than version 5.0.

The vSphere Authentication Proxy service binds to an IPv4 address for communication with vCenter Server, and does not support IPv6. The vCenter Server can be on a host machine in an IPv4-only, IPv4/IPv6 mixed-mode, or IPv6-only network environment, but the machine that connects to the vCenter Server through the vSphere Web Client must have an IPv4 address for the vSphere Authentication Proxy service to work.

Prerequisites

- Install vSphere Auto Deploy. See "Install or Upgrade vSphere Auto Deploy," on page 131.
- Verify that you have administrator privileges.
- Verify that the host machine has Windows Installer 3.0 or later.
- Verify that the host machine has a supported processor and operating system. vSphere Authentication Proxy supports the same processors and operating systems as vCenter Server. See "vCenter Server Software Requirements," on page 22 and "Hardware Requirements for vCenter Server, the vSphere Web Client, vCenter Inventory Service, and vCenter Single Sign-On," on page 17.
- Verify that the host machine has a valid IPv4 address. You can install vSphere Authentication Proxy on a machine in an IPv4-only or IPv4/IPv6 mixed-mode network environment, but you cannot install vSphere Authentication Proxy on a machine in an IPv6-only environment.
- If you are installing vSphere Authentication Proxy on a Windows Server 2008 R2 host machine, download and install the Windows hotfix described in Windows KB Article 981506 on the support.microsoft.com Web site. If this hotfix is not installed, the vSphere Authentication Proxy Adapter fails to initialize. This problem is accompanied by error messages in `camadapter.log` similar to `Failed to bind CAM website with CTL` and `Failed to initialize CAMAdapter.`

Gather the following information to complete the installation or upgrade:

- The location to install vSphere Authentication Proxy, if you are not using the default location.
- The address and credentials for the vCenter Server that vSphere Authentication Proxy will connect to: IP address or name, HTTP port, user name, and password.
- The host name or IP address to identify vSphere Authentication Proxy on the network.

Procedure

1. On the host machine where you will install the vSphere Authentication Proxy service, install the .NET Framework 3.5.
2. Install vSphere Auto Deploy.

   You do not have to install Auto Deploy on the same host machine as the vSphere Authentication Proxy service.
3. Add the host machine where you will install the authentication proxy service to the domain.
4. Use the Domain Administrator account to log in to the host machine.
5. In the software installer directory, double-click the `autorun.exe` file to start the installer.
6. Select **vSphere Authentication Proxy** and click **Install**.
7. Follow the wizard prompts to complete the installation or upgrade.

   During installation, the authentication service registers with the vCenter Server instance where Auto Deploy is registered.

When you install the vSphere Authentication Proxy service, the installer creates a domain account with appropriate privileges to run the authentication proxy service. The account name begins with the prefix `CAM–` and has a 32-character, randomly generated password associated with it. The password is set to never expire. Do not change the account settings.

What to do next

Configure ESXi to use vSphere Authentication Proxy to join a domain. See the *vSphere Security* documentation.

Enable IPv6 Support for vCenter Inventory Service

vCenter Inventory Service does not support binding on IPv6 interfaces by default. When you install vCenter Server, vCenter Inventory Service supports only IPv4 by default. You can enable IPv6 support for vCenter Inventory Service by modifying the Inventory Service `dataservice.properties` file.

Procedure

1 Stop the vCenter Inventory Service.

   a From the Administrative Tools control panel, select **Services**.

   b Right-click **vCenter Inventory Service** and select **Stop**.

2 In a text editor, open the file:*`Inventory_Service_installation_directory`*`/lib/server/config/dataservice.properties`.

3 Change the line `dataservice.nio.enabled = true` to `dataservice.nio.enabled = false`

4 Restart the vCenter Inventory Service.

IPv6 support for vCenter Inventory Service is enabled.

Linked Mode Considerations for vCenter Server

Consider several issues before you configure a Linked Mode group.

Before you configure a Linked Mode group, consider the following issues.

- If you are upgrading a version 5.x vCenter Server that is part of a Linked Mode group, it will not be removed from the group. If you are upgrading a pre-5.0 vCenter Server that is part of a Linked Mode group, it will be removed from the group. vCenter Server does not support Linked Mode groups that contain both version 5.x and pre-5.0 versions of vCenter Server. Similarly, vCenter Server does not support Linked Mode groups that contain different 5.x versions of vCenter Server or different versions of vCenter Single Sign-On. After all 5.x vCenter Server and vCenter Single Sign-On instances in a Linked Mode group are upgraded to the same 5.x version, you can rejoin them.
- Each vCenter Server user sees the vCenter Server instances on which they have valid permissions.
- When you set up your vCenter Server Linked Mode group, you must install the first vCenter Server as a standalone instance because you do not yet have a remote vCenter Server machine to join. Subsequent vCenter Server instances can join the first vCenter Server or other vCenter Server instances that have joined the Linked Mode group.
- If you join a vCenter Server to a standalone instance that is not part of a domain, you must add the standalone instance to a domain and add a domain user as an administrator.
- The vCenter Server instances in a Linked Mode group do not need to have the same domain user login. The instances can run under different domain accounts. By default, they run as the LocalSystem account of the machine on which they are running, which means that they are different accounts.
- During vCenter Server installation, if you enter an IP address for the remote instance of vCenter Server, the installer converts it into a fully qualified domain name.

CAUTION If you need to uninstall and reinstall vCenter Server on more than one member of a Linked Mode group, do so with a single vCenter Server at a time. Uninstalling and reinstalling multiple linked vCenter Servers at the same time is not supported, and can cause errors that prevent vCenter Server from connecting to vCenter Inventory Service. If it is necessary to uninstall and reinstall multiple linked vCenter Servers at the same time, isolate them from the Linked Mode group first, and rejoin them to the Linked Mode group after the reinstallation is complete.

Linked Mode Prerequisites for vCenter Server

Prepare the vCenter Server system for joining a Linked Mode group.

Before joining a vCenter Server to a Linked Mode group, review "Linked Mode Considerations for vCenter Server," on page 134.

All the requirements for standalone vCenter Server systems apply to Linked Mode systems.

The following requirements apply to each vCenter Server system that is a member of a Linked Mode group:

- vCenter Server does not support Linked Mode groups that contain both version 5.x and pre-5.0 versions of vCenter Server. Similarly, vCenter Server does not support Linked Mode groups that contain different 5.x versions of vCenter Server or different versions of vCenter Single Sign-On. After all 5.x vCenter Server and vCenter Single Sign-On instances in a Linked Mode group are upgraded to the same 5.x version, you can rejoin them.
- Make sure that all vCenter Servers in a Linked Mode group are registered to the same vCenter Single Sign-On server.
- To join a vCenter Server to another vCenter Server in Linked Mode, the currently logged-in user who is performing the join operation must have access to the vCenter Server database of each vCenter Server.
- When you join a vCenter Server instance to a Linked Mode group, the installer must be run by a domain user who is an administrator on both the machine where vCenter Server is installed and the target machine of the Linked Mode group.
- When you join a vCenter Server instance to a Linked Mode group, if User Account Control (UAC) is enabled on the machine, the join operation requires elevated privileges through the **Run as administrator** option. This is true even if the logged-in user is a domain administrator user.
- To join a Linked Mode group the vCenter Server must be in evaluation mode or licensed as a Standard edition. vCenter Server Foundation and vCenter Server Essentials editions do not support Linked Mode.
- DNS must be operational for Linked Mode replication to work.
- The vCenter Server instances in a Linked Mode group can be in different domains if the domains have a two-way trust relationship. Each domain must trust the other domains on which vCenter Server instances are installed.
- All vCenter Server instances must have network time synchronization. The vCenter Server installer validates that the machine clocks are not more than five minutes apart. See "Synchronizing Clocks on the vSphere Network," on page 53.

Join a Linked Mode Group After a vCenter Server Upgrade

After you upgrade to vCenter Server 5.5, you can join the system to a Linked Mode group. A Linked Mode group allows you to log in to any single instance of vCenter Server in the group and view and manage the inventories of all the vCenter Server systems in the group.

Prerequisites

See "Linked Mode Prerequisites for vCenter Server," on page 135.

NOTE vCenter Server does not support Linked Mode groups that contain both version 5.x and pre-5.0 versions of vCenter Server. Similarly, vCenter Server does not support Linked Mode groups that contain different 5.x versions of vCenter Server or different versions of vCenter Single Sign-On. After all 5.x vCenter Server and vCenter Single Sign-On instances in a Linked Mode group are upgraded to the same 5.x version, you can rejoin them.

Procedure

1 From the **Start** menu, select **All Programs > VMware > vCenter Server Linked Mode Configuration**.

2 Click **Next**.

3 Select **Modify linked mode configuration** and click **Next**.

4 Click **Join vCenter Server instance to an existing linked mode group or another instance** and click **Next**.

5 Type the server name and LDAP port number of any remote vCenter Server that is or will be a member of the group and click **Next**.

If you enter an IP address, the installer converts it to a fully qualified domain name.

6 If the vCenter Server installer detects a role conflict, select how to resolve the conflict.

A conflict results if the joining system and the Linked Mode group each contain a role with the same name but with different privileges.

Option	Description
Yes, let VMware vCenter Server resolve the conflicts for me	Click **Next**. The role on the joining system is renamed to *vcenter_namerole_name* where *vcenter_name* is the name of the vCenter Server system that is joining the Linked Mode group and *role_name* is the name of the original role.
No, I'll resolve the conflicts myself	To resolve the conflicts manually: a Using the vSphere Web Client, log in to the vCenter Server system that is joining the Linked Mode group using an account with Administrator privileges. b Rename the conflicting role. c Close the vSphere Web Client session and return to the vCenter Server installer. d Click **Back**, and click **Next**. The installation continues without conflicts.

7 Click **Finish**.

vCenter Server restarts. Depending on the size of your inventory, the change to Linked Mode might take from a few seconds to a few minutes to complete.

The vCenter Server instance is now part of a Linked Mode group. It might take several seconds for the global data (such as user roles) that are changed on one machine to be visible on the other machines. The delay is usually 15 seconds or less. It might take a few minutes for a new vCenter Server instance to be recognized and published by the existing instances, because group members do not read the global data very often.

After you form a Linked Mode group, you can log in to any single instance of vCenter Server and view and manage the inventories of all the vCenter Servers in the group.

What to do next

For information about Linked Mode groups, see the *vCenter Server and Host Management* documentation.

Configuring VMware vCenter Server - tc Server Settings in vCenter Server

Starting with vCenter Server 5.1, VMware Tomcat Server settings can no longer be configured through the Windows user interface. vCenter Server versions 5.1 and later use VMware vCenter Server - tc Server, an enterprise version of Apache Tomcat 7. Tomcat version 7 does not provide a control panel in the Windows user interface. Instead, you configure Tomcat by editing configuration files manually.

You can adjust the JVM maximum heap size for vCenter Server, vCenter Inventory Service, and Profile-Driven Storage Service. For JVM heap size recommendations, see "Hardware Requirements for vCenter Server, the vSphere Web Client, vCenter Inventory Service, and vCenter Single Sign-On," on page 17.

Settings for Java options are stored in the following files.

- vCenter Server. *installation_directory*\VMware\Infrastructure\tomcat\conf\wrapper.conf
- vCenter Inventory Service. *installation_directory*\VMware\Infrastructure\Inventory Service\conf\wrapper.conf
- Profile-Driven Storage Service. *installation_directory*\VMware\Infrastructure\Profile-Driven Storage\conf\wrapper.conf
- The vSphere Web Client. *installation_directory*\VMware\vSphereWebClient\server\bin\service\conf\wrapper.conf

Table 5-2. Inventory Service and Profile-Driven Storage Service Java Maximum JVM Heap Size Setting in the `wrapper.conf` Files

Java Option	Setting and Default Value
`maxmemory`*size* The maximum JVM heap size, in megabytes. This setting controls the maximum size of the Java heap. Tuning this parameter can reduce the overhead of garbage collection, improving server response time and throughput. For some applications, the default setting for this option is too low, resulting in a high number of minor garbage collections.	Inventory Service: `wrapper.java.maxmemory=2048` Profile-Driven Storage Service: `wrapper.java.maxmemory=1024` The vSphere Web Client: For large deployments you might need to set this option to `wrapper.java.maxmemory=2048`
`ping.timeout`*duration*	The vSphere Web Client: For large deployments you might need to set this option to `wrapper.ping.timeout=120`

vCenter Server security and port settings are stored in the following files.

- *installation_directory*\VMware\Infrastructure\tomcat\conf\server.xml
- *installation_directory*\VMware\Infrastructure\tomcat\conf\catalina.properties

Table 5-3. vCenter Server Port and Security Settings in the `server.xml` and `catalina.properties` Files

vCenter Server Port or Security Setting	Setting and Default Value
Base shutdown port	base.shutdown.port=8003
Base JMX port. The listener implemented by the com.springsource.tcserver.serviceability.rmi.JmxSocketListener class is specific to tc Server. This listener enables JMX management of tc Server, and is the JMX configuration that the AMS management console uses to manage tc Server instances. The port attribute specifies the port of the JMX server that management products, such as AMS, connect to. The variable *${jmx.port}* is set to 6969 in the default `catalina.properties` file. The bind attribute specifies the host of the JMX server. By default, this attribute is set to the localhost (127.0.0.1). The default -1 setting disables the port.	base.jmx.port=-1

Table 5-3. vCenter Server Port and Security Settings in the `server.xml` and `catalina.properties` Files (Continued)

vCenter Server Port or Security Setting	Setting and Default Value
Web services HTTPS	bio-vmssl.http.port=8080
Web services HTTPS	bio-vmssl.https.port=8443
SSL certificate	bio-vmssl.keyFile.name=C:\ProgramData\VMware\VMware VirtualCenter\SSL\rui.pfx
SSL certificate password	bio-vmssl.SSL.password=testpassword
AJP port	bio-vmssl.ajp.port=8009

See *Getting Started with vFabric tc Server* and *vFabric tc Server Administration* at https://www.vmware.com/support/pubs/vfabric-tcserver.html.

You can manage the Windows services for vCenter Server from the Administrative Tools control panel, under Services. The Windows service for vCenter Server is listed as VMware VirtualCenter Management Webservices.

Set the Maximum Number of Database Connections After a vCenter Server Upgrade

By default, a vCenter Server creates a maximum of 50 simultaneous database connections. If you configure this value to less than 50 in the previous version of vCenter Server and then perform the upgrade to vCenter Server 5.x, the upgrade restores the default setting of 50. If you configure this value to more than 50 in the previous version of vCenter Server, after the upgrade to vCenter Server 5.x, the system retains the previous value. You can reconfigure the nondefault setting.

You might want to increase the number of database connections if the vCenter Server frequently performs many operations and performance is critical. You might want to decrease this number if the database is shared and connections to the database are costly. Do not change this value unless your system has one of these problems.

Perform this task before you configure the authentication for your database. For more information about configuring authentication, see the documentation for your database.

Procedure

1 From the vSphere Web Client, connect to the vCenter Server.

2 Select the vCenter Server in the inventory.

3 Click the **Manage** tab.

4 Select **Settings**.

5 Select **General**.

6 Click **Edit**.

7 Select **Database**.

8 Change the **Maximum connections** value as appropriate.

9 Click **OK**.

10 Restart the vCenter Server.

The new database setting takes effect.

Upgrading Update Manager 6

You can upgrade to Update Manager 5.5 from Update Manager version 4.x, Update Manager 5.0 and Update Manager 5.1 that are installed on a 64-bit operating system. Direct upgrades from Update Manager 1.0 Update 6 and earlier, and Update Manager systems that are installed on a 32-bit platform are not supported.

If you are running an earlier version of Update Manager on a 32-bit platform, you cannot perform an in-place upgrade to Update Manager 5.5. You must use the data migration tool that is provided with Update Manager 5.0 installation media to move your Update Manager system from 32-bit operating system to Update Manager 5.0 on a 64-bit operating system, and then perform an in-place upgrade from version 5.0 to version 5.5. For detailed information how to use the data migration tool, see the *Installing and Administering VMware vSphere Update Manager* documentation for Update Manager 5.0.

When you upgrade Update Manager, you cannot change the installation path and patch download location. To change these parameters, you must install a new version of Update Manager rather than upgrade.

Previous versions of Update Manager use a 512-bit key and self-signed certificate and these are not replaced during upgrade. If you require a more secure 2048-bit key, you can either perform a fresh installation of Update Manager 5.5, or use the Update Manager Utility to replace the existing certificate.

Scheduled tasks for virtual machine patch scan and remediation are not removed during the upgrade. After the upgrade, you can edit and remove scheduled scan tasks that exist from previous releases. You can remove existing scheduled remediation tasks but you cannot edit them.

Virtual machine patch baselines are removed during the upgrade. Existing scheduled tasks that contain them run normally and ignore only the scanning and remediation operations that use virtual machine patch baselines.

You must upgrade the Update Manager database during the Update Manager upgrade. You can select whether to keep your existing data in the database or to replace it during the upgrade.

The Java Components (JRE) required by Update Manager are installed or upgraded silently on the system when you install or upgrade Update Manager. Starting with Update Manager 5.5 update 1, you can upgrade the Java Components separately to a version that is released asynchronously from Update Manager releases.

This chapter includes the following topics:

Upgrade the Update Manager Server

To upgrade an instance of Update Manager that is installed on a 64-bit machine, you must first upgrade vCenter Server to a compatible version.

The Update Manager 5.5 release allows upgrades from Update Manager 1.0 Update 6, Update Manager 4.x, Update Manager 5.0, and Update Manager 5.1.

Prerequisites

- Ensure that you grant the database user the required set of privileges. See the *Preparing the Update Manager Database* chapter in *Installing and Administering VMware vSphere Update Manager*.
- Stop the Update Manager service and back up the Update Manager database. The installer upgrades the database schema, making the database irreversibly incompatible with previous Update Manager versions.

Procedure

1 Upgrade vCenter Server to a compatible version.

NOTE The vCenter Server installation wizard warns you that Update Manager is not compatible when vCenter Server is upgraded.

If prompted, you must restart the machine that is running vCenter Server. Otherwise, you might not be able to upgrade Update Manager.

2 In the software installer directory, double-click the `autorun.exe` file at `C:\installer_location`, and select **vSphere Update Manager**.

If you cannot launch the `autorun.exe` file, browse to locate the `UpdateManager` folder and run `VMware-UpdateManager.exe`.

3 Select a language and click **OK**.

4 In the upgrade warning message, click **OK**.

5 Review the Welcome page and click **Next**.

6 Read the patent agreement and click **Next**.

7 Accept the terms in the license agreement and click **Next**.

8 Review the support information, select whether to delete old upgrade files, select whether to download updates from the default download sources immediately after installation, and click **Next**.

If you deselect **Delete the old host upgrade files from the repository**, you retain files that you cannot use with Update Manager 5.5.

If you deselect **Download updates from default sources immediately after installation**, Update Manager downloads updates once daily according to the default download schedule or immediately after you click **Download Now** on the Download Settings page. You can modify the default download schedule after the installation is complete.

9 Type the vCenter Server system credentials and click **Next**.

To keep the Update Manager registration with the original vCenter Server system valid, keep the vCenter Server system IP address and enter the credentials from the original installation.

10 Type the database password for the Update Manager database and click **Next**.

The database password is required only if the DSN does not use Windows NT authentication.

11 On the Database Upgrade page, select **Yes, I want to upgrade my Update Manager database** and **I have taken a backup of the existing Update Manager database**, and click **Next**.

12 (Optional) On the Database re-initialization warning page, select to keep your existing remote database if it is already upgraded to the latest schema.

If you replace your existing database with an empty one, you lose all of your existing data.

13 Specify the Update Manager port settings, select whether you want to configure the proxy settings, and click **Next**.

Configure the proxy settings if the computer on which Update Manager is installed has access to the Internet.

14 (Optional) Provide information about the proxy server and port, specify whether the proxy should be authenticated, and click **Next**.

15 Click **Install** to begin the upgrade.

16 Click **Finish**.

You upgraded the Update Manager server.

What to do next

Upgrade the Update Manager Client plug-in.

Upgrade the Update Manager Client Plug-In

The Update Manager server and the Update Manager Client plug-in must be of the same version.

Prerequisites

Upgrade the Update Manager server.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered.

2 Select **Plug-ins > Manage Plug-ins**.

3 In the Plug-in Manager window, click **Download and install** for the VMware vSphere Update Manager extension.

4 Complete the Update Manager Client installation, and click **Finish**.

The status for the Update Manager extension is displayed as Enabled.

5 Click **Close** to close the Plug-in Manager window.

The icon for the Update Manager Client plug-in is displayed on the vSphere Client Home page.

Upgrading and Migrating Your Hosts 7

After you upgrade vCenter Server, and vSphere Update Manager if you are using Update Manager, upgrade or migrate VMware ESX 4.x and ESXi 4.x hosts, or update ESXi 5.0.x hosts, to ESXi 5.x.

These topics are intended for administrators who are upgrading ESX, ESXi, and virtual machines from ESX 4.x/ESXi 4.x, or updating ESXi 5.0.x, to ESXi 5.x.

This chapter includes the following topics:

Preparing to Upgrade Hosts

For a successful upgrade of your hosts, understand and prepare for the changes that are involved.

Best Practices for ESXi Upgrades and Migrations

When you upgrade or migrate hosts, you must understand and follow the best practices process for a successful upgrade or migration.

For a successful upgrade or migration, follow these best practices:

1. Make sure that you understand the ESXi upgrade process, the effect of that process on your existing deployment, and the preparation required for the upgrade.
   - If your vSphere system includes VMware solutions or plug-ins, make sure they are compatible with the vCenter Server version that you are upgrading to. See the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.
   - Read "Preparing to Upgrade Hosts," on page 143 to understand the changes in configuration and partitioning between ESX/ESXi 4.x and ESXi 5.x, the upgrade and migration scenarios that are supported, and the options and tools available to perform the upgrade or migration.
   - Read the VMware vSphere Release Notes for known installation issues.
   - If your vSphere installation is in a VMware View environment, see "Upgrading vSphere Components Separately in a Horizon View Environment," on page 220.
2. Prepare your system for the upgrade.
   - Make sure your current ESX or ESXi version is supported for migration or upgrade. See "Supported Upgrades to ESXi 5.5.x," on page 152.

- Make sure your system hardware complies with ESXi requirements. See Chapter 2, "System Requirements," on page 13 and the VMware Compatibility Guide, at http://www.vmware.com/resources/compatibility/search.php. Check for system compatibility, I/O compatibility (network and HBA cards), storage compatibility, and backup software compatibility.
- Make sure that sufficient disk space is available on the host for the upgrade or migration. Migrating from ESX 4.x to ESXi 5.x requires 50MB of free space on your VMFS datastore.
- If a SAN is connected to the host, detach the fibre before continuing with the upgrade or migration. Do not disable HBA cards in the BIOS.

  NOTE This step does not apply to ESX hosts that boot from the SAN and have the Service Console on the on the SAN LUNs. You can disconnect LUNs that contain the VMFS datastore and do not contain the Service Console.

3 Back up your host before performing an upgrade or migration, so that, if the upgrade fails, you can restore your host.

   IMPORTANT Once you have upgraded or migrated your host to ESXi 5.x, you cannot roll back to your version 4.x ESX or ESXi software.

4 Depending on the upgrade or migration method you choose, you might need to migrate or power off all virtual machines on the host. See the instructions for your upgrade or migration method.

5 After the upgrade or migration, test the system to ensure that the upgrade or migration completed successfully.

6 Reapply your host licenses. See "Reapplying Licenses After Upgrading to ESXi 5.5," on page 214.

7 Consider setting up a syslog server for remote logging, to ensure sufficient disk storage for log files. Setting up logging on a remote host is especially important for hosts with limited local storage. Optionally, you can install the vSphere Syslog Collector to collect logs from all hosts. See "Providing Sufficient Space for System Logging," on page 23. For information about setting up and configuring syslog and a syslog server, setting up syslog from the host profiles interface, and installing vSphere Syslog Collector, see the *vSphere Installation and Setup* documentation.

8 If the upgrade or migration was unsuccessful, and you backed up your host, you can restore your host.

Files and Configuration Settings Affected by the Migration or Upgrade from ESX 4.x or ESXi 4.x to ESXi 5.x

The migration or upgrade from ESX 4.x or ESXi 4.x to ESXi 5.x does not migrate all host configuration files and settings.

After the upgrade, you must reconfigure some host settings.

Migrating ESX 4.x Files and Settings to ESXi 5.x

The upgrade process preserves as much of the ESX host configuration as possible. However, because of the architectural differences between ESX 4.x and ESXi 5.x architecture, many configuration files cannot be migrated when you select the **Migrate** option in the ESXi installation or upgrade wizard.

Pertinent VMware files, such as `/etc/vmware/esx.conf` are migrated, but many existing settings such as third-party agents and scripts, cannot be migrated.

NOTE If a 4.x host contains customizations, such as third-party VIBS or drivers, upgrading with the standard VMware installer ISO will result in the loss of those customizations, and possibly an unstable system. Use ESXi Image Builder CLI to create a customized ESXi installer ISO file that includes the VIBs or drivers. See the information on Image Builder in the *vSphere Installation and Setup* documentation.

Table 7-1. Files Migrated During Migration or Upgrade to ESXi

File Migrated	Comments
/etc/sfcb/sfcb.cfg	Migrated.
/var/lib/sfcb/registration/repository/root/interop/*	Migrated.
/etc/logrotate.conf	Not migrated. ESXi Logrotation is incompatible with prior versions.
/etc/localtime	Not migrated. Timezones are not supported in ESXi.
/etc/ntp.conf	Migrated.
/etc/ntp.drift	Migrated.
/etc/ntp.keys	Migrated.
/etc/syslog.conf	Migrated for ESXi, not migrated for ESX.
/etc/security/access.conf	Migrated. Needed for PAM configurations.
/etc/security/login.map	
/etc/sysconfig/network	Migrated. Service Console virtual NICs (vswifs) will be converted to ESXi virtual NICs. (vmks)
/etc/sysconfig/ntp	Not migrated.
/etc/sysconfig/xinetd	Not migrated.
/etc/sysconfig/console/*	Not migrated.
/etc/sysconfig/i18n	Not migrated. i18n is not supported in ESXi
/etc/sysconfig/clock	Not migrated. Timezones are not supported in ESXi.
/etc/sysconfig/crond	Not migrated.
/etc/sysconfig/syslog	Not migrated. The syslog daemon is incompatible with prior versions.
/etc/sysconfig/keyboard	Migrated. Any entries not supported will default to English.
/etc/sysconfig/mouse	Not migrated. No mouse support in ESXi.
/etc/sysconfig/static-routes	Migrated.
/etc/sysconfig/static-routes-ipv6	Migrated.
/etc/sysconfig/network-scripts/route-$device	Migrated.
/etc/ssh	Not migrated. See "SSH Configuration Affected by Upgrading or Migrating to ESXi 5.x," on page 147.
/etc/nsswitch.conf	Migrated. Used generically for various configurations, most helpful for Active Directory authentication.
/etc/yp.conf	Not migrated. NIS is not supported in ESXi.
/etc/krb.conf	Needed for Likewise to have Active Directory support.
/etc/krb.realms	
/etc/krb5.conf	
/etc/krb5.acl	
/etc/krb5.keytab	
/etc/krb5.log	
/etc/krb5.mkey	

Table 7-1. Files Migrated During Migration or Upgrade to ESXi (Continued)

File Migrated	Comments
/etc/login.defs	Not migrated. This file controls settings like maildir, password aging controls, uid and gid min/max settings, and the user deletion command.
/etc/pam.d/*	Partially migrated. Needed for authentication and authorization. **Note** Custom edits made to settings in /etc/pam.d/system-auth in ESX 4.x are reset to the default values by the upgrade to ESXi 5.x. To maintain the custom values, reset them manually after the upgrade.
/etc/hosts.allow	Not migrated.
/etc/hosts.deny	Not migrated.
/etc/ldap.conf	Not migrated. LDAP is not supported in ESXi.
/etc/openldap	
/etc/sudoers	Not migrated. SUDO is not supported in ESXi.
/etc/snmp/snmpd.conf	Migrated to /etc/vmware/snmp.xml.
/usr/local/etc/	Not migrated.
/etc/rc.d/rc*.d/*	Not migrated. ESX and ESXi rc.d scripts are incompatible.
/etc/xinetd.conf	Not migrated. xinetd is not supported in ESXi.
/etc/motd	Migrated. A note is appended saying the system was upgraded to ESX 5.x
/etc/likewise/*	Migrated. Used for Likewise configurations.
/etc/vmware/vmkiscsid/*	Migrated.
etc/vmware/init/*	Not migrated. Init scripts are incompatible.
/etc/vmware/esx.conf	Migrated.
/etc/vmware/pci*	Not migrated.
/etc/vmware/simple.map	Not migrated. A new simple.map file is generated.
/etc/vmware/license.cfg	Not migrated. The valuation mode timer is be reset on upgrades.
/etc/vmware/vmware.lic	Not migrated. ESXi 5.x upgrades are reset to evaluation mode.
/etc/vmware/hostd/*	Migrated.
/etc/vmware/hostd/config.xml	Not migrated. This file is currently incompatible with ESXi.
/etc/vmware/hostd/proxy.xml	Not migrated. This file is currently incompatible with ESXi.
/etc/vmware/vmauth/authentication.conf	Migrated. Used for Likewise configurations.
/etc/vmware/vmauth/provider.xml	
/etc/hosts	Migrated.
/etc/resolv.conf	Migrated.
/usr/lib/vmware	Not migrated.
/etc/fstab	Partially migrated. Only NFS entries will be migrated to ESXi.
/etc/passwd	Partially migrated. Only the root user password will be saved, if possible.

Table 7-1. Files Migrated During Migration or Upgrade to ESXi (Continued)

File Migrated	Comments
`/etc/shadow`	
`/etc/groups`	Not migrated.

Firewall Configuration Changes After Migration or Upgrade to ESXi 5.x

The migration or upgrade from ESX/ESXi 4.x to ESXi 5.x results in several changes to the host firewall configuration.

When you migrate from ESX 4.x to ESXi 5.x, the ESX 4.x rulesets list is replaced by the new rulesets list in ESXi 5.x. The following configuration from the `/etc/vmware/esx.conf` file is preserved:

- The existing enabled/disabled status.
- The allowedip added by `esxcfg-firewall`.

Ruleset files that are added by the user and customized firewall rules created in ESX 4.x. are not preserved after the migration. In the first boot after the migration, for those rulesets that don't have entries in the ESX 4.x `/etc/vmware/esx.conf` file, the ESXi 5.x firewall loads the default enabled status.

After the migration to ESXi 5.x, the default block policy is set to false (PASS all traffic by default) on ESXi 5.x only when both blockIncoming and blockOutgoing values of the default policy are false in the ESX 4.x `/etc/vmware/esx.conf` file. Otherwise the default policy is to deny all traffic.

Custom ports that were opened by using the ESX/ESXi 4.1 `esxcfg-firewall` command do not remain open after the upgrade to ESXi 5.x. The configuration entries are ported to the `esx.conf` file by the upgrade, but the corresponding ports are not opened. See the information about ESXi firewall configuration in the *vSphere Security* documentation.

Important The ESXi firewall in ESXi 5.x does not allow per-network filtering of vMotion traffic. Therefore, you must install rules on your external firewall to ensure that no incoming connections can be made to the vMotion socket.

Resource Pool Settings Affected by the Upgrade from ESX 4.x to ESXi 5.x

After the upgrade to ESXi 5.x, ESX 4.x resource pool settings might be insufficient to start all virtual machines in the pool.

The upgrade to ESXi 5.x affects the amount of memory available to the host system. As a result, in resource pools that are set to use nearly all of the resources available, some virtual machines might not have enough resources to start after the upgrade. When this happens, a system alert will be issued. You can find this alert by pressing Alt + F11 in the ESXi direct console. Reconfigure the resource pools to solve the problem.

SSH Configuration Affected by Upgrading or Migrating to ESXi 5.x

The host SSH configuration is migrated only for upgrades from ESXi 4.1 or ESXi 5.0 x to ESXi 5.x

SSH configuration is not migrated for ESX 4.x hosts or ESXi 4.0 hosts. For these hosts, SSH access is disabled during the upgrade or migration process. You can reenable SSH access in the direct console. See the information on enabling SSH access in the *vSphere Installation and Setup* documentation.

Networking Changes in ESXi 5.x

Some ESX 4.x and ESXi 4.x network settings stored in `/etc/sysconfig/network` are migrated in the upgrade or migration to ESXi 5.x. In the migration to ESXi 5.x, ESX Service Console virtual NICs (vswifs) are converted to ESXi virtual NICs (vmks).

The distributed port group or dvPort that the virtual NICs connect to is also migrated. The Service Console port group is renamed as the Management Network port group. When vswifs are migrated to vmks, they are numbered to follow any existing vmk in sequence. For example, if the version 4.x ESX host has virtual NICs vmk0, vmk1, and vswif0, after the migration the new ESXi configuration will be vmk0, vmk1, and vmk2, where vmk2 is the management interface.

When virtual NICs are configured to use DHCP, a setting controls whether DHCP sets the default route and host name in addition to installing an IPv4 address. In ESX this setting is PEERDNS. In ESXi, the setting is DhcpDNS. The PEERDNS value for ESX Service Console virtual NICs is migrated to the DhcpDNS setting for the ESXi virtual NICs. The DhcpDNS setting preserves the ESX configuration for default route and host name as well as the IPv4 address.

The migration from ESX 4.x to ESXi 5.x also preserves manually assigned IPv4 and IPv6 addresses, default route, and host-specific IPv4 and IPv6 routes.

When you upgrade from ESXi 4.x to ESXi 5.x, the default maximum number of ports for a virtual switch changes from 64 to 128. To keep the same maximum number of ports that you have in ESXi 4.x, set the value explicitly before you upgrade, using the vSphere Web Client.

ESX hosts have two IP stacks, one for the vmkernel and one for the Service Console. Because ESXi hosts have only one IP stack, the migration cannot preserve both ESX default routes. After migration, the ESX Service Console default route becomes the single ESXi default route, replacing the vmkernel route. The change to a single ESXi default route might cause loss of connectivity for routed nonmanagement traffic that originates from vmkernel. To restore vmkernel networking, you can configure static routes in addition to the default route.

All vswif interfaces are migrated to vmk interfaces. If a conflict is detected between two interfaces, one is left in disabled state. The upgrade disables any conflicting kernel IP addressing in favor of the management interface.

The migration to ESXi 5.x disables any existing vmk virtual NIC that meets the following conditions.

- The vmk virtual NIC has a manually configured (static) IP address.
- The IP address is in the same subnet as a vswif virtual NIC that is being migrated to a switch containing the vmk virtual NIC.
- The vmk and vswif NICs are both on the same virtual switch.

For example, if vswif0, with IP address 192.0.2.1/24 on vswitch1, is migrated to a switch containing vmk0, with IP address 192.0.2.2/24, also on vswitch1, after the migration, vmk0 will be disabled.

ESX 4.x Service Console Port Group Removed in Migration to ESXi 5.x

Because ESXi 5.x has no Service Console, migrating from ESX 4.x to ESXi 5.x removes the Service Console port group.

After the migration to ESXi 5.x, a new port group, the Management Network port group, is created.

If any of your ESX hosts require the Service Console port group to support an existing service, you can write a firstboot script to recreate the port group after the migration. See the information on the `%firstboot` command in "Installation and Upgrade Script Commands," on page 185.

Partitioning Changes from ESX 4.x to ESXi 5.x

The ESXi partition scheme used in ESXi 5.x differs from that of earlier ESX and ESXi versions. ESXi 5.x does not have the Service Console partition found in ESX.

How these changes affect your host depends on whether you are upgrading to ESXi 5.x or performing a fresh installation.

Partitioning in New ESXi 5.x Installations

In new installations, several new partitions are created for the boot banks, the scratch partition, and the locker. New ESXi 5.x installations use GUID Partition Tables (GPT) instead of MSDOS-based partitioning.

The partition table is fixed as part of the binary image, and is written to the disk at the time the system is installed. The ESXi installer leaves the scratch and VMFS partitions blank, and ESXi creates them when the host is rebooted for the first time after installation or upgrade. The scratch partition is 4GB. The rest of the disk is formatted as a VMFS5 partition.

NOTE The installer can create multiple VFAT partitions. The VFAT designation does not always indicate that the partition is a scratch partition. In some cases, a VFAT partition can lie idle.

Partitioning in Upgraded ESXi 5.x Hosts

Upgraded systems do not use GUID Partition Tables (GPT), but retain the older MSDOS-based partition label.

For most ESXi 4.x hosts, the partition table is not rewritten in the upgrade to ESXi 5.x. The partition table is rewritten for systems that have lopsided bootbanks. Lopsided boot banks can occur in systems that are upgraded from ESXi 3.5 to ESXi 4.x, and then upgraded directly to ESXi 5.x.

For ESX hosts, the partitioning structure is changed to resemble that of an ESXi 4.x host. The VMFS3 partition is retained and a new MSDOS-based partition table overwrites the existing partition table.

For ESX hosts, any data stored in custom user created partitions inside the Service Console is not preserved in the migration to ESXi 5.x.

Upgraded hosts do not have a scratch partition. Instead, the scratch directory is created and accessed off of the VMFS volume. Each of the other partitions, such as the bootbanks, locker and vmkcore are identical to that of any other system.

In upgraded hosts, the VMFS partition is not upgraded from VMFS3 to VMFS5. ESXi 5.x is compatible with VMFS3 partitions. You can upgrade the partition to VMFS5 after the host is upgraded to ESXi 5.x. See the information on upgrading datastores to VMFS5 in the *vSphere Storage* documentation.

Upgraded hosts, which keep the older MSDOS-based partitioning, do not support installing ESXi on a single physical disk or LUN larger than 2TB. To install ESXi on a disk or LUN larger than 2TB, you must do a fresh installation.

NOTE The ESXi 5.x installer cannot detect ESX 2.x instances or VMFS2 datastores. You cannot migrate ESX 2.x instances to ESXi 5.x or preserve VMFS2 datastores in an upgrade to ESXi 5.x. Instead, perform a fresh installation of ESXi 5.x.

For the VMFS partition on the disk to be preserved during an upgrade to ESXi 5.x, the partition must be physically located after the boot partition, which is partition 4, and the extended partition on the disk (8192 + 1835008 sectors). Any system that has a VMFS partition after the 1843200 sector mark can keep that VMFS partition, regardless of whether it was initially installed with ESX 3.5 or 4.x.

For systems in which the VMFS partition is placed on a different drive from the boot drive, the entire contents of the boot drive is overwritten during the upgrade. Any extra data on the disk is erased.

ESXi 5.5 Upgrade Options

VMware provides several ways to upgrade ESX/ESXi hosts.

vSphere Update Manager

vSphere Update Manager is software for upgrading, migrating, updating, and patching clustered hosts, virtual machines, and guest operating systems. Update Manager orchestrates host and virtual machine upgrades. If your site uses vCenter Server, VMware recommends that you use Update Manager. For instructions about conducting an orchestrated host upgrade, see "Using vSphere Update Manager to Perform Orchestrated Host Upgrades," on page 166. For instructions about conducting an orchestrated virtual machine upgrade, see the *Installing and Administering VMware vSphere Update Manager* documentation.

Upgrade or migrate interactively using an ESXi installer ISO image on CD/DVD or USB flash drive

You can run the ESXi 5.5.x installer from a CD/DVD or USB flash drive to do an interactive upgrade or migration. This method is appropriate for deployments with a small number of hosts. The installer works the same as for a fresh installation, but if you select a target disk that already contains an ESX/ESXi 4.x, ESXi 5.0.x, ESXi 5.1.x, or ESXi 5.5.0 installation, the installer upgrades the host to 5.5.x, and gives you the option to migrate some existing host settings and configuration files, and preserve the existing VMFS datastore. See "Upgrade or Migrate Hosts Interactively," on page 180.

Perform a scripted upgrade

You can upgrade or migrate hosts from version 4.x ESXi and ESX, version 5.0.x ESXi, version 5.1.x ESXi, and version 5.5.0 ESXi to ESXi 5.5.x by invoking an update script, for an efficient, unattended upgrade. Scripted upgrades provide an efficient way to deploy multiple hosts. You can use a script to upgrade ESXi from a CD, DVD or USB flash drive, or by PXE-booting the installer. You can also call a script from an interactive installation. See "Installing, Upgrading, or Migrating Hosts Using a Script," on page 182.

vSphere Auto Deploy

Auto Deploy is a new feature in vSphere 5.x. After an ESXi 5.x host is deployed with Auto Deploy, you can use Auto Deploy to reprovision the host and reboot it with a new image profile that contains an ESXi upgrade or patch, a host configuration profile, and, optionally, third-party drivers or management agents provided by VMware partners. You can build custom images by using ESXi Image Builder CLI. See "Using vSphere Auto Deploy to Reprovision Hosts," on page 196.

esxcli

You can use the `esxcli` command-line utility for ESXi to upgrade ESXi 5.0.x hosts or ESXi 5.1.x hosts to ESXi 5.5.x. You cannot use `esxcli` to upgrade ESX/ESXi 4.x hosts to ESXi 5.5.x. The `esxcli` command-line utility requires the vSphere CLI. See "Upgrading Hosts by Using esxcli Commands," on page 200.

The `esxupdate` and `vihostupdate` utilities are not supported for ESXi 5.x upgrades.

Table 7-2. ESXi 5.5.x Upgrade Methods

Upgrade Method	Upgrade from ESX or ESXi 4.x to ESXi 5.5.x	Upgrade from ESXi 5.0.x to ESXi 5.5.x	Upgrade from ESXi 5.1.x to ESXi 5.5.x	Upgrade from ESXi 5.5.0 to ESXi 5.5.x
vSphere Update Manager	yes	yes	yes	yes
Interactive upgrade from CD, DVD, or USB drive	yes	yes	yes	yes
Scripted upgrade	yes	yes	yes	yes
vSphere Auto Deploy	no	yes, if the ESXi 5.0.x host was deployed using Auto Deploy	yes, if the ESXi 5.1.x host was deployed using Auto Deploy	yes, if the ESXi 5.5.0 host was deployed using Auto Deploy
esxcli	no	yes	yes	yes

Upgrading Hosts That Have Third-Party Custom VIBs

When you upgrade a host that contains custom VIBs, the upgrade displays an error message unless the same VIBs are included in the upgrade ISO file.

A host can have custom VIBs installed, for example, for third-party drivers or management agents. For example, ESX/ESXi 4.x hosts can contain Cisco Nexus 1000V VEMs or EMC PowerPath modules. The ESXi 5.x architecture differs from ESX/ESXi 4.x so that customized third-party software packages (VIBs) cannot be migrated when you upgrade from ESX/ESXi 4.x to ESXi 5.x. When you upgrade a 4.x host with custom VIBs that are not in the upgrade ISO, the ESXi installer displays an error message that lists the missing VIBs.

To migrate the third-party customizations as part of the host upgrade, use ESXi Image Builder to create a custom ESXi ISO image that includes the missing VIBs. For information about using Image Builder to make a custom ISO, see the information about Using ESXi Image Builder in the *vSphere Installation and Setup* documentation.

To upgrade a version 4.x ESX/ESXi host, without including the third-party software, you can take one of the following actions.

- Remove the third-party software. If you are using vSphere Update Manager, select the option to remove third-party software modules during the remediation process. For information about upgrading with vSphere Update Manager, see *Installing and Administering VMware vSphere Update Manager*.
- Override the error message during the host upgrade by selecting the Force Migrate option.

Caution Using either of these two options might cause the upgraded host to not boot properly, to exhibit system instability, or to lose functionality. Ensure that your system does not have any critical dependence on third-party VIBs that requires resolution on first boot and cannot be resolved later. For example, your system might require custom drivers for NICs that you are booting from.

If you are upgrading a 5.0.x host, supported custom VIBs on the host that are not included in the ESXi installer ISO are migrated. If the host or the installer .ISO contains a VIB that creates a conflict and prevents the upgrade, an error message identifies the offending VIB. You can remove the VIB and retry the upgrade, or use ESXI Image Builder CLI to create a custom installer .ISO that resolves the conflict. The `forcemigrate` option is not available.

If you are upgrading a host running ESX/ESXi 4.1 Upgrade 1 or ESX/ESXi 4.0 Upgrade 3, you will see the error message for the VIBs listed in Table 7-3, even if you have never installed any custom VIBs. If you are sure that the proper functioning or your system does not depend on those VIBs, you can choose to ignore the warnings and continue with the upgrade.

Table 7-3. ESX/ESXi 4.0 U3 and 4.1 U1 Third-Party VIBs That Cannot Be Migrated to ESXi 5.x.

ESX/ESXi Release	Bulletin ID	VIB ID
4.1 Upgrade 1	ESX410-201101224-UG	cross_vmware-esx-drivers-net-vxge_400.2.0.28.21239-1OEM If your system does not include any hardware that requires this Neterion driver, you can ignore the error message.
4.1 Upgrade 1	ESX410-201101223-UG	cross_vmware-esx-drivers-scsi-3w-9xxx_400.2.26.08.036vm40-1OEM If your system does not include any hardware that requires this 3ware driver, you can ignore the error message.
4.0 Upgrade 3	ESX400-201105213-UG	cross_vmware-esx-drivers-scsi-3w-9xxx_400.2.26.08.036vm40-1OEM If your system does not include any hardware that requires this 3ware driver, you can ignore the error message.

Supported Upgrades to ESXi 5.5.x

You can upgrade an ESXi 5.0.x, ESXi 5.1.x, or ESXi 5.5.0 host directly to 5.5.x, and in most cases, you can migrate an ESX 4.x or upgrade an ESXi 4.x host directly to 5.5.x.

The details and level of support for an upgrade or migration to 5.5.x depend on the host to be upgraded and the upgrade method that you use. Verify support for the upgrade path from your current version of ESX or ESXi to the version that you are upgrading to. See the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Table 7-4. Supported Scenarios for Upgrade or Migration to 5.5.x.

Scenario for Upgrade or Migration to 5.5.x	Support
3.x ESX and ESXi hosts	Not supported for direct upgrade. You must upgrade version 3.x ESX and ESXi hosts to ESX or ESXi version 4.x before you can upgrade them to 5.5.x. See the vSphere 4.x upgrade documentation. Alternatively, you might find it simpler and more cost effective to do a fresh installation of 5.5.x.
4.x ESX host that was upgraded from ESX 3.x with a partition layout incompatible with ESXi 5.x	Not supported. The VMFS partition cannot be preserved. Upgrading or migration is possible only if there is at most one VMFS partition on the disk that is being upgraded and the VMFS partition must start after sector 1843200. Perform a fresh installation. To keep virtual machines, migrate them to a different system.
4.x ESX or ESXi host, migration or upgrade with vSphere Update Manager	Supported. See "Using vSphere Update Manager to Perform Orchestrated Host Upgrades," on page 166 and the *Installing and Administering VMware vSphere Update Manager* documentation.

Table 7-4. Supported Scenarios for Upgrade or Migration to 5.5.x. (Continued)

Scenario for Upgrade or Migration to 5.5.x	Support
4.x ESX or ESXi host, interactive migration or upgrade	Supported. See "Upgrade or Migrate Hosts Interactively," on page 180. The installer wizard offers the choice to upgrade or perform a fresh installation. If you upgrade, ESX partitions and configuration files are converted to be compatible with ESXi.
4.x ESX or ESXi host, scripted upgrade	Supported. See "Installing, Upgrading, or Migrating Hosts Using a Script," on page 182. In the upgrade script, specify the particular disk to upgrade on the system. If the system cannot be upgraded correctly because the partition table is incompatible, the installer displays a warning and does not proceed. In this case, perform a fresh installation. Upgrading or migration is possible only if there is at most one VMFS partition on the disk that is being upgraded and the VMFS partition must start after sector 1843200.
4.x ESX host on a SAN or SSD	Partially supported. You can upgrade the host as you would a normal ESX 4.x host, but no provisions will be made to optimize the partitions on the disk. To optimize the partition scheme on the host, perform a fresh installation.
4.x ESX host, missing Service Console `.vmdk` file, interactive migration from CD or DVD, scripted migration, or migration with vSphere Update Manager	Not supported. The most likely reasons for a missing Service Console are that the Service Console is corrupted or that the VMFS volume is not available, which can occur if the VMFS was installed on a SAN and the LUN is not accessible. In this case, on the disk selection screen of the installer wizard, if you select a disk that has an existing ESX 4.x installation, the wizard prompts you to perform a clean installation.
4.x ESX or ESXi host, asynchronously released driver or other third-party customizations, interactive migration from CD or DVD, scripted migration, or migration with vSphere Update Manager	Supported with ESXi Image Builder CLI. If a 4.x host contains customizations, such as third-party VIBS or drivers, upgrading with the standard VMware installer ISO will result in the loss of those customizations, and possibly an unstable system. See "Upgrading Hosts That Have Third-Party Custom VIBs," on page 151. You can ESXi Image Builder CLI to create a customized ESXi installer ISO file that includes the VIBs or drivers. See the information on Image Builder in the *vSphere Installation and Setup* documentation.
5.0.x or 5.1.x ESXi host, asynchronously released driver or other third-party customizations, interactive upgrade from CD or DVD, scripted upgrade, or upgrade with vSphere Update Manager	Supported. When you upgrade an ESXi 5.0.x or 5.1.x host that has custom VIBs to version 5.5, the custom VIBs are migrated. See "Upgrading Hosts That Have Third-Party Custom VIBs," on page 151.
5.0.x ESXi host	Methods supported for direct upgrade to 5.5.x are: ■ vSphere Update Manager. ■ Interactive upgrade from CD, DVD, or USB drive. ■ Scripted upgrade. ■ Auto Deploy. If the ESXi 5.0.x host was deployed using Auto Deploy, you can use Auto Deploy to reprovision the host with an 5.5.x image. ■ esxcli.

Table 7-4. Supported Scenarios for Upgrade or Migration to 5.5.x. (Continued)

Scenario for Upgrade or Migration to 5.5.x	Support
5.1.x ESXi host	Methods supported for direct upgrade to 5.5.x are: ■ vSphere Update Manager. ■ Interactive upgrade from CD, DVD, or USB drive. ■ Scripted upgrade. ■ Auto Deploy. If the ESXi 5.1.x host was deployed using Auto Deploy, you can use Auto Deploy to reprovision the host with an 5.5.x image. ■ esxcli.
5.5.0 ESXi host	Methods supported for direct upgrade to 5.5.x are: ■ vSphere Update Manager. ■ Interactive upgrade from CD, DVD, or USB drive. ■ Scripted upgrade. ■ Auto Deploy. If the ESXi 5.5.0 host was deployed using Auto Deploy, you can use Auto Deploy to reprovision the host with an 5.5.x image. ■ esxcli.

Using Manually Assigned IP Addresses for Upgrades and Migrations Performed with vSphere Update Manager

If you are using vSphere Update Manager to upgrade or migrate a host from ESX/ESXi 4.x to ESXi 5.x, you must use manually assigned IP addresses for the hosts. Manually assigned IP addresses also referred to as static IP addresses.

DHCP IP addresses can cause problems during host upgrades or migrations performed with Update Manager. If a host loses its DHCP IP address during an upgrade or migration because the lease period configured on the DHCP server expires, Update Manager loses connectivity to the host. In this case, even if the host upgrade or migration is successful, Update Manager reports the upgrade or migration as failed, because it cannot connect to the host. To prevent this scenario, use manually assigned IP addresses for your hosts.

Media Options for Booting the ESXi Installer

The ESXi installer must be accessible to the system on which you are installing ESXi.

The following boot media are supported for the ESXi installer:

- Boot from a CD/DVD. See "Download and Burn the ESXi Installer ISO Image to a CD or DVD," on page 154.
- Boot from a USB flash drive. See "Format a USB Flash Drive to Boot the ESXi Installation or Upgrade," on page 155.
- PXE boot from the network. "PXE Booting the ESXi Installer," on page 158
- Boot from a remote location using a remote management application. See "Using Remote Management Applications," on page 165

Download and Burn the ESXi Installer ISO Image to a CD or DVD

If you do not have an ESXi installation CD/DVD, you can create one.

You can also create an installer ISO image that includes a custom installation script. See "Create an Installer ISO Image with a Custom Installation or Upgrade Script," on page 157.

Procedure

1 Download the ESXi installer from the VMware Web site at https://my.vmware.com/web/vmware/downloads.

ESXi is listed under Datacenter & Cloud Infrastructure.

2 Confirm that the md5sum is correct.

See the VMware Web site topic Using MD5 Checksums at http://www.vmware.com/download/md5.html.

3 Burn the ISO image to a CD or DVD.

Format a USB Flash Drive to Boot the ESXi Installation or Upgrade

You can format a USB flash drive to boot the ESXi installation or upgrade.

These instructions assume that you are performing the procedure on a Linux machine and that the USB flash drive is detected by the operating system as `/dev/sdb`.

NOTE The `ks` file containing the installation script cannot be located on the same USB flash drive that you are using to boot the installation or upgrade.

Prerequisites

- From the VMware Web site, download the ESXi ISO image `VMware-VMvisor-Installer-5.x.x-XXXXXX.x86_64.iso`, including the file `isolinux.cfg`, where *5.x.x* is the version of ESXi you are installing, and *XXXXXX* is the build number of the installer ISO image.
- Verify that the machine on which you are performing this procedure has access to syslinux version 3.86. This procedure requires syslinux version 3.86.

Procedure

1 If your USB flash drive is not detected as `/dev/sdb`, or you are not sure how your USB flash drive is detected, determine how it is detected.

a In a terminal window, run the following command.

```
tail -f /var/log/messages
```

This command displays current log messages in the terminal window.

b Plug in your USB flash drive.

The terminal window displays several messages identifying the USB flash drive, in a format similar to the following message.

```
Oct 25 13:25:23 ubuntu kernel: [  712.447080] sd 3:0:0:0: [sdb] Attached SCSI removable disk
```

In this example, "[sdb]" identifies the USB device. If your device is identified differently, use that identification, without the brackets, in place of sdb, in this procedure.

2 Create a partition table on the USB flash device.

```
/sbin/fdisk /dev/sdb
```

a Type `d` to delete partitions until they are all deleted.

b Type `n` to create primary partition 1 that extends over the entire disk.

c Type `t` to set the type to an appropriate setting for the FAT32 file system, such as **c**.

d Type `a` to set the active flag on partition 1.

e Type `p` to print the partition table.

The result should be similar to the following text:

```
Disk /dev/sdb: 2004 MB, 2004877312 bytes
255 heads, 63 sectors/track, 243 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1               1         243      1951866  c   W95 FAT32 (LBA)
```

f Type `w` to write the partition table and quit.

3 Format the USB flash drive with the Fat32 file system.

```
/sbin/mkfs.vfat -F 32 -n USB /dev/sdb1
```

4 Run the following commands.

```
/path_to_syslinux-3.86_directory/syslinux-3.86/bin/syslinux /dev/sdb1
cat /path_to_syslinux-3.86_directory/syslinux-3.86/usr/share/syslinux/mbr.bin > /dev/sdb
```

5 Mount the USB flash drive.

```
mount /dev/sdb1 /usbdisk
```

6 Mount the ESXi installer ISO image.

```
mount -o loop VMware-VMvisor-Installer-5.x.x-XXXXXX.x86_64.iso /esxi_cdrom
```

7 Copy the contents of the ISO image to `/usbdisk`.

```
cp -r /esxi_cdrom/* /usbdisk
```

8 Rename the `isolinux.cfg` file to `syslinux.cfg`.

```
mv /usbdisk/isolinux.cfg /usbdisk/syslinux.cfg
```

9 In the file `/usbdisk/syslinux.cfg`, change the line `APPEND -c boot.cfg` to `APPEND -c boot.cfg -p 1`.

10 Unmount the USB flash drive.

```
umount /usbdisk
```

11 Unmount the installer ISO image.

```
umount /esxi_cdrom
```

The USB flash drive can now boot the ESXi installer.

Create a USB Flash Drive to Store the ESXi Installation Script or Upgrade Script

You can use a USB flash drive to store the ESXi installation script or upgrade script that is used during scripted installation or upgrade of ESXi.

When multiple USB flash drives are present on the installation machine, the installation software searches for the installation or upgrade script on all attached USB flash drives.

The instructions in this procedure assume that the USB flash drive is detected as `/dev/sdb`.

NOTE The `ks` file containing the installation or upgrade script cannot be located on the same USB flash drive that you are using to boot the installation or upgrade.

Prerequisites

- Linux machine
- ESXi installation or upgrade script, the `ks.cfg` kickstart file

- USB flash drive

Procedure

1 Attach the USB flash drive to a Linux machine that has access to the installation or upgrade script.

2 Create a partition table.

```
/sbin/fdisk /dev/sdb
```

   a Type `d` to delete partitions until they are all deleted.

   b Type `n` to create primary partition 1 that extends over the entire disk.

   c Type `t` to set the type to an appropriate setting for the FAT32 file system, such as **c**.

   d Type `p` to print the partition table.

   The result should be similar to the following text:

```
Disk /dev/sdb: 2004 MB, 2004877312 bytes
255 heads, 63 sectors/track, 243 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1               1         243      1951866  c   W95 FAT32 (LBA)
```

   e Type `w` to write the partition table and quit.

3 Format the USB flash drive with the Fat32 file system.

```
/sbin/mkfs.vfat –F 32 –n USB /dev/sdb1
```

4 Mount the USB flash drive.

```
mount /dev/sdb1 /usbdisk
```

5 Copy the ESXi installation script to the USB flash drive.

```
cp ks.cfg /usbdisk
```

6 Unmount the USB flash drive.

The USB flash drive contains the installation or upgrade script for ESXi.

What to do next

When you boot the ESXi installer, point to the location of the USB flash drive for the installation or upgrade script. See "Enter Boot Options to Start an Installation or Upgrade Script," on page 182 and "About PXE Configuration Files," on page 161.

Create an Installer ISO Image with a Custom Installation or Upgrade Script

You can customize the standard ESXi installer ISO image with your own installation or upgrade script. This enables you to perform a scripted, unattended installation or upgrade when you boot the resulting installer ISO image.

See also "About Installation and Upgrade Scripts," on page 184 and "About the boot.cfg File," on page 193.

Prerequisites

- Linux machine.
- The ESXi ISO image `VMware-VMvisor-Installer-`*`5.x.x-XXXXXX`*`.x86_64.iso`,where *`5.x.x`* is the version of ESXi you are installing, and *XXXXXX* is the build number of the installer ISO image.
- Your custom installation or upgrade script, the `ks_cust.cfg` kickstart file.

Procedure

1 Download the ESXi ISO image from the VMware Web site.

2 Mount the ISO image into a folder:

```
mount -o loop VMware-VMvisor-Installer-5.x.x-XXXXXX.x86_64.iso /esxi_cdrom_mount
```

XXXXXX is the ESXi build number for the version that you are installing or upgrading to.

3 Copy the contents of `cdrom` to another folder:

```
cp -r /esxi_cdrom_mount /esxi_cdrom
```

4 Copy the kickstart file to `/esxi_cdrom`

```
cp ks_cust.cfg /esxi_cdrom
```

5 (Optional) Modify the `boot.cfg` file to specify the location of the installation or upgrade script using the `kernelopt` option.

This step makes the installation or upgrade completely automatic, without the need to specify the kickstart file during the installation or upgrade.

6 Recreate the ISO image:

```
mkisofs -relaxed-filenames -J -R -o custom_esxi.iso -b isolinux.bin -c boot.cat -no-emul-boot
-boot-load-size 4 -boot-info-table /esxi_cdrom
```

The ISO image now includes your custom installation or upgrade script.

What to do next

Install ESXi from the ISO image.

PXE Booting the ESXi Installer

You use the preboot execution environment (PXE) to boot a host and launch the ESXi installer from a network interface.

ESXi 5.x is distributed in an ISO format that is designed to install to flash memory or to a local hard drive. You can extract the files and boot using PXE.

PXE uses DHCP and Trivial File Transfer Protocol (TFTP) to boot an operating system over a network.

PXE booting requires some network infrastructure and a machine with a PXE-capable network adapter. Most machines that are capable of running ESXi have network adapters that are able to PXE boot.

NOTE Ensure that the Auto Deploy server has an IPv4 address. PXE booting is supported only with IPv4.

About the TFTP Server, PXELINUX, and gPXE

Trivial File Transfer Protocol (TFTP) is similar to the FTP service, and is typically used only for network booting systems or loading firmware on network devices such as routers.

Most Linux distributions include a copy of the tftp-hpa server. If you require a supported solution, purchase a supported TFTP server from your vendor of choice.

If your TFTP server will run on a Microsoft Windows host, use tftpd32 version 2.11 or later. See http://tftpd32.jounin.net/. Earlier versions of tftpd32 were incompatible with PXELINUX and gPXE.

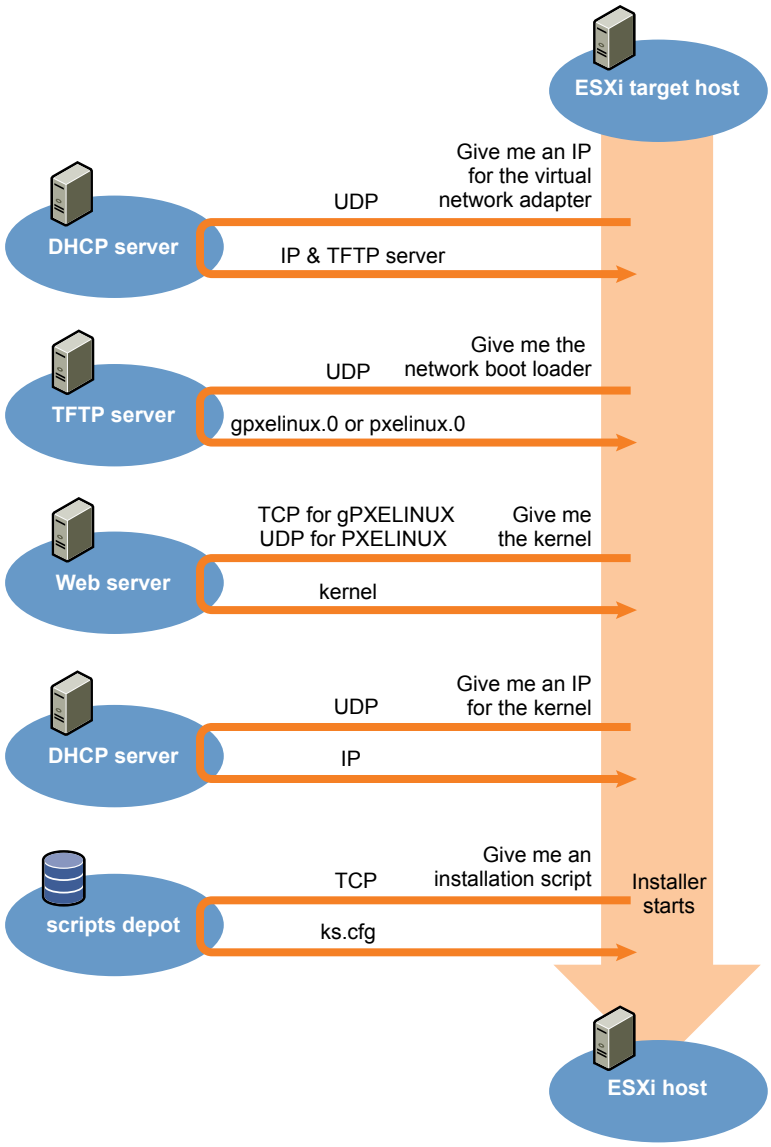
You can also acquire a TFTP server from one of the packaged appliances on the VMware Marketplace.

The PXELINUX and gPXE environments allow your target machine to boot the ESXi installer. PXELINUX is part of the SYSLINUX package, which can be found at http://www.kernel.org/pub/linux/utils/boot/syslinux/, although many Linux distributions include it. Many versions of PXELINUX also include gPXE. Some distributions, such as Red Hat Enterprise Linux version 5.3, include earlier versions of PXELINUX that do not include gPXE.

If you do not use gPXE, you might experience problems while booting the ESXi installer on a heavily loaded network TFTP is sometimes unreliable for transferring large amounts of data. If you use PXELINUX without gPXE, the `pxelinux.0` binary file, the configuration file, the kernel, and other files are transferred by TFTP. If you use gPXE, only the `gpxelinux.0` binary file and configuration file are transferred by TFTP. With gPXE, you can use a Web server to transfer the kernel and other files required to boot the ESXi installer.

NOTE VMware tests PXE booting with PXELINUX version 3.86. This is not a statement of limited support. For support of third-party agents that you use to set up your PXE booting infrastructure, contact the vendor.

Figure 7-1. Overview of PXE Boot Installation Process



Sample DHCP Configuration

To PXE boot the ESXi installer, the DHCP server must send the address of the TFTP server and a pointer to the `pxelinux.0` or `gpxelinux.0` directory.

The DHCP server is used by the target machine to obtain an IP address. The DHCP server must be able to determine whether the target machine is allowed to boot and the location of the PXELINUX binary (which usually resides on a TFTP server). When the target machine first boots, it broadcasts a packet across the network requesting this information to boot itself. The DHCP server responds.

CAUTION Do not set up a new DHCP server if your network already has one. If multiple DHCP servers respond to DHCP requests, machines can obtain incorrect or conflicting IP addresses, or can fail to receive the proper boot information. Talk to a network administrator before setting up a DHCP server. For support on configuring DHCP, contact your DHCP server vendor.

Many DHCP servers can PXE boot hosts. If you are using a version of DHCP for Microsoft Windows, see the DHCP server documentation to determine how to pass the `next-server` and `filename` arguments to the target machine.

gPXE Example

This example shows how to configure a ISC DHCP version 3.0 server to enable gPXE.

```
allow booting;
allow bootp;
# gPXE options
option space gpxe;
option gpxe-encap-opts code 175 = encapsulate gpxe;
option gpxe.bus-id code 177 = string;
class "pxeclients" {
   match if substring(option vendor-class-identifier, 0, 9) = "PXEClient";
   next-server TFTP server address;
   if not exists gpxe.bus-id {
      filename "/gpxelinux.0";
   }
}
subnet Network address netmask Subnet Mask {
   range Starting IP Address Ending IP Address;
}
```

When a machine attempts to PXE boot, the DHCP server provides an IP address and the location of the `gpxelinux.0` binary file on the TFTP server. The IP address assigned is in the range defined in the subnet section of the configuration file.

PXELINUX (without gPXE) Example

This example shows how to configure a ISC DHCP version 3.0 server to enable PXELINUX.

```
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.sample
#
ddns-update-style ad-hoc;
allow booting;
allow bootp;
class "pxeclients" {
   match if substring(option vendor-class-identifier, 0, 9) = "PXEClient";
   next-server xxx.xxx.xx.xx;
```

```
   filename = "pxelinux.0";
}
subnet 192.168.48.0 netmask 255.255.255.0 {
   range 192.168.48.100 192.168.48.250;
}
```

When a machine attempts to PXE boot, the DHCP server provides an IP address and the location of the `pxelinux.0` binary file on the TFTP server. The IP address assigned is in the range defined in the subnet section of the configuration file.

About PXE Configuration Files

The PXE configuration file defines the menu displayed to the target ESXi host as it boots up and contacts the TFTP server. You need a PXE configuration file to PXE boot the ESXi installer.

The TFTP server constantly listens for PXE clients on the network. When it detects that a PXE client is requesting PXE services, it sends the client a network package that contains a boot menu.

Required Files

In the PXE configuration file, you must include paths to the following files:

- `mboot.c32` is the boot loader.
- `boot.cfg` is the boot loader configuration file.

See "About the boot.cfg File," on page 193

File Name for the PXE Configuration File

For the file name of the PXE configuration file, select one of the following options:

- `01-`*`mac_address_of_target_ESXi_host`*. For example, `01-23-45-67-89-0a-bc`
- The target ESXi host IP address in hexadecimal notation.
- `default`

The initial boot file, `pxelinux.0` or `gpxelinux.0`, tries to load a PXE configuration file. It tries with the MAC address of the target ESXi host, prefixed with its ARP type code, which is 01 for Ethernet. If that attempt fails, it tries with the hexadecimal notation of target ESXi system IP address. Ultimately, it tries to load a file named `default`.

File Location for the PXE Configuration File

Save the file in `var/lib/tftpboot/pxelinux.cfg/` on the TFTP server.

For example, you might save the file on the TFTP server at `/tftpboot/pxelinux.cfg/01-00-21-5a-ce-40-f6`. The MAC address of the network adapter on the target ESXi host is 00-21-5a-ce-40-f6.

PXE Boot the ESXi Installer by Using PXELINUX and a PXE Configuration File

You can use a TFTP server to PXE boot the ESXi installer, using PXELINUX and a PXE configuration file.

See also "About Installation and Upgrade Scripts," on page 184 and "About the boot.cfg File," on page 193

Prerequisites

Verify that your environment has the following components:

- The ESXi installer ISO image downloaded from the VMware Web site.
- TFTP server that supports PXE booting with gPXE. See "About the TFTP Server, PXELINUX, and gPXE," on page 158.
- DHCP server configured for PXE booting. See "Sample DHCP Configuration," on page 160.

- PXELINUX
- Server with a hardware configuration that is supported with your version of ESXi. See the Hardware Compatibility Guide at http://www.vmware.com/resources/compatibility/search.php.
- Network security policies to allow TFTP traffic (UDP port 69)
- (Optional) Installation script, the kickstart file. See "About Installation and Upgrade Scripts," on page 184.
- Network adapter with PXE support on the target ESXi host
- IPv4 networking. IPv6 is not supported for PXE booting.

Use a native VLAN in most cases. If you want to specify the VLAN ID to be used with PXE booting, check that your NIC supports VLAN ID specification.

Procedure

1 Create the `/tftpboot/pxelinux.cfg` directory on your TFTP server.

2 On the Linux machine, install PXELINUX.

PXELINUX is included in the SYSLINUX package. Extract the files, locate the `pxelinux.0` file and copy it to the `/tftpboot` directory on your TFTP server.

3 Configure the DHCP server to send the following information to each client host:

- The name or IP address of your TFTP server.
- The name of your initial boot file. This is `pxelinux.0`.

4 Copy the contents of the ESXi installer image to the `/var/lib/tftpboot` directory on the TFTP server.

5 (Optional) For a scripted installation, in the `boot.cfg` file, add the `kernelopt` option on the line following the kernel command, to specify the location of the installation script.

Use the following code as a model, where `XXX.XXX.XXX.XXX` is the IP address of the server where the installation script resides, and `esxi_ksFiles` is the directory containing the `ks.cfg` file.

```
kernelopt=ks=http://XXX.XXX.XXX.XXX/esxi_ksFiles/ks.cfg
```

6 Create a PXE configuration file.

This file defines how the host boots when no operating system is present. The PXE configuration file references the boot files. Use the following code as a model, where `XXXXXX` is the build number of the ESXi installer image.

```
DEFAULT menu.c32
MENU TITLE ESXi-5.x.x-XXXXXX-full Boot Menu
NOHALT 1
PROMPT 0
TIMEOUT 80
LABEL install
  KERNEL mboot.c32
   APPEND -c location of boot.cfg
MENU LABEL ESXi-5.x.x-XXXXXX-full ^Installer
LABEL hddboot
 LOCALBOOT 0x80
 MENU LABEL ^Boot from local disk
```

7 Name the file with the MAC address of the target host machine: `01-mac_address_of_target_ESXi_host`.

For example, `01-23-45-67-89-0a-bc`.

8 Save the PXE configuration file in `/tftpboot/pxelinux.cfg` on the TFTP server.

9 Boot the machine with the network adapter.

PXE Boot the ESXi Installer by Using PXELINUX and an isolinux.cfg PXE Configuration File

You can PXE boot the ESXi installer using PXELINUX, and use the isolinux.cfg file as the PXE configuration file.

See also "About Installation and Upgrade Scripts," on page 184 and "About the boot.cfg File," on page 193

Prerequisites

Verify that your environment has the following components:

- The ESXi installer ISO image downloaded from the VMware Web site.
- TFTP server that supports PXE booting with PXELINUX. See "About the TFTP Server, PXELINUX, and gPXE," on page 158.
- DHCP server configured for PXE booting. See "Sample DHCP Configuration," on page 160.
- PXELINUX
- Server with a hardware configuration that is supported with your version of ESXi. See the *Hardware Compatibility Guide* at http://www.vmware.com/resources/compatibility/search.php.
- Network security policies to allow TFTP traffic (UDP port 69)
- (Optional) Installation script, the kickstart file. See "About Installation and Upgrade Scripts," on page 184.
- Network adapter with PXE support on the target ESXi host
- IPv4 networking. IPv6 is not supported for PXE booting.

Use a native VLAN in most cases. If you want to specify the VLAN ID to be used with PXE booting, check that your NIC supports VLAN ID specification.

Procedure

1 Create the `/tftpboot/pxelinux.cfg` directory on your TFTP server.

2 On the Linux machine, install PXELINUX.

PXELINUX is included in the SYSLINUX package. Extract the files, locate the file `pxelinux.0` and copy it to the `/tftpboot` directory on your TFTP server.

3 Configure the DHCP server.

The DHCP server sends the following information to your client hosts:

- The name or IP address of your TFTP server.
- The name of your initial boot file. This is `pxelinux.0`.

4 Copy the contents of the ESXi installer image to the `/var/lib/tftpboot` directory on the TFTP server.

5 (Optional) For a scripted installation, in the `boot.cfg` file, add the `kernelopt` option on the next line after the `kernel` command, to specify the location fo the installation script.

In the following example, *XXX.XXX.XXX.XXX* is the IP address of the server where the installation script resides.

```
kernelopt=ks=http://XXX.XXX.XXX.XXX/esxi_ksFiles/ks.cfg
```

6 Copy the `isolinux.cfg` file from the ESXi installer ISO image to the `/tftpboot/pxelinux.cfg` directory.

The `isolinux.cfg` file contains the following code, where `XXXXXX` is the build number of the ESXi installer image:

```
DEFAULT menu.c32
MENU TITLE ESXi-5.x.x-XXXXXX-full Boot Menu
NOHALT 1
PROMPT 0
TIMEOUT 80
LABEL install
  KERNEL mboot.c32
   APPEND -c location of boot.cfg
MENU LABEL ESXi-5.x.x-XXXXXX-full ^Installer
LABEL hddboot
 LOCALBOOT 0x80
 MENU LABEL ^Boot from local disk
```

7 Rename the `isolinux.cfg` file with the MAC address of the target host machine: `01-mac_address_of_target_ESXi_host`. For example, `01-23-45-67-89-0a-bc`

8 Boot the machine with the network adapter.

PXE Boot the ESXi Installer Using gPXE

You can PXE boot the ESXi installer using gPXE.

See also "About Installation and Upgrade Scripts," on page 184 and "About the boot.cfg File," on page 193

Prerequisites

Verify that your environment has the following components:

- The ESXi installer ISO image downloaded from the VMware Web site
- HTTP Web server that is accessible by your target ESXi hosts
- DHCP server configured for PXE booting: `/etc/dhcpd.conf` is configured for client hosts with a TFTP server and the initial boot file set to `gpxelinux.0/undionly.kpxe`. See "Sample DHCP Configuration," on page 160.
- Server with a hardware configuration that is supported with your version of ESXi. See the Hardware Compatibility Guide at http://www.vmware.com/resources/compatibility/search.php.
- gPXELINUX
- (Optional) ESXi installation script. See "About Installation and Upgrade Scripts," on page 184.

Use a native VLAN in most cases. If you want to specify the VLAN ID to be used with PXE booting, check that your NIC supports VLAN ID specification.

Procedure

1 Copy the contents of the ESXi installer ISO image to the `/var/www/html` directory on the HTTP server.

2 Modify the `boot.cfg` file with the information for the HTTP server.

Use the following code as a model, where *XXX.XXX.XXX.XXX* is the HTTP server IP address. The `kernelopt` line is optional. Include that option to specify the location of the installation script for a scripted installation.

```
title=Loading ESX installer
kernel=http://XXX.XXX.XXX.XXX/tboot.b00
kernelopt=ks=http://XXX.XXX.XXX.XXX/esxi_ksFiles/ks.cfg
modules=http://XXX.XXX.XXX.XXX/b.b00 --- http://XXX.XXX.XXX.XXX/useropts.gz ---
```

```
http://XXX.XXX.XXX.XXX/k.b00 --- http://XXX.XXX.XXX.XXX/a.b00 ---
http://XXX.XXX.XXX.XXX/s.v00 --- http://XXX.XXX.XXX.XXX/weaselin.t00 ---
http://XXX.XXX.XXX.XXX/tools.t00 --- http://XXX.XXX.XXX.XXX/imgdb.tgz ---
http://XXX.XXX.XXX.XXX/imgpayld.tgz
```

3 gPXE boot the host and press Ctrl+B to access the GPT menu.

4 Enter the following commands to boot with the ESXi installer, where *XXX.XXX.XXX.XXX* is the HTTP server IP address.

```
dhcp net0 ( if dchp is not set)
kernel –n mboot.c32 http://XXX.XXX.XXX.XXX/mboot.c32
imgargs mboot.c32 –c http://XXX.XXX.XXX.XXX/boot.cfg
boot mboot.c32
```

Installing and Booting ESXi with Software FCoE

You can install and boot ESXi from an FCoE LUN using VMware software FCoE adapters and network adapters with FCoE offload capabilities. Your host does not require a dedicated FCoE HBA.

See the *vSphere Storage* documentation for information about installing and booting ESXi with software FCoE.

Using Remote Management Applications

Remote management applications allow you to install ESXi on servers that are in remote locations.

Remote management applications supported for installation include HP Integrated Lights-Out (iLO), Dell Remote Access Card (DRAC), IBM management module (MM), and Remote Supervisor Adapter II (RSA II). For a list of currently supported server models and remote management firmware versions, see "Supported Remote Management Server Models and Minimum Firmware Versions," on page 28. For support on remote management applications, contact the vendor.

You can use remote management applications to do both interactive and scripted installations of ESXi remotely.

If you use remote management applications to install ESXi, the virtual CD might encounter corruption problems with systems or networks operating at peak capacity. If a remote installation from an ISO image fails, complete the installation from the physical CD media.

Download the ESXi Installer

Download the installer for ESXi.

Prerequisites

Create a My VMware account at https://my.vmware.com/web/vmware/.

Procedure

1 Download the ESXi installer from the VMware Web site at https://my.vmware.com/web/vmware/downloads.

ESXi is listed under Datacenter & Cloud Infrastructure.

2 Confirm that the md5sum is correct.

See the VMware Web site topic Using MD5 Checksums at http://www.vmware.com/download/md5.html.

Performing the Upgrade or Migration

Several tools are available to upgrade and migrate hosts. You can use different upgrade tools based depending on the type of host you are upgrading (ESX or ESXi) and whether the hosts are managed by vCenter Server.

You can migrate or upgrade to ESXi 5.x from version 4.x ESX or ESXi or version 5.0.x with the tools and methods described in "ESXi 5.5 Upgrade Options," on page 150.

To upgrade version 3.5 ESX or ESXi to ESXi 5.x, you must first upgrade version 3.5 ESX or ESXi to version 4.x ESX or ESXi. See the VMware vSphere 4.x documentation Web page for information about upgrading from version 3.5 ESX or ESXi 3.5 to version 4.x ESX or ESXi.

Caution If you upgrade hosts managed by vCenter Server, you must upgrade to vCenter Server before you upgrade ESX or ESXi. If you do not upgrade in the correct order, you can lose data and lose access to your servers.

Using vSphere Update Manager to Perform Orchestrated Host Upgrades

Orchestrated upgrades allow you to upgrade the objects in your vSphere inventory in a two-step process: host upgrades, followed by virtual machine upgrades. You can configure the process at the cluster level to automate more of the process, or you can configure it at the individual host or virtual machine level for granular control.

For example, you can define a host upgrade baseline to upgrade an ESXi 4.x host to ESXi 5.x, or you can define a virtual machine upgrade baseline to upgrade the VMware Tools and the virtual machine hardware to the latest version. Use wizard-based workflows to first schedule host upgrades for an entire cluster and then schedule a virtual machine upgrade for all the virtual machines.

You cannot use Update Manager to upgrade a host to ESXi 5.x if the host was previously upgraded from ESX 3.x to ESX 4.x. Such hosts do not have sufficient free space in the /boot partition to support the Update Manager upgrade process. This problem also affects some 4.x ESX hosts, even if they were not previously upgraded from ESX 3.x. Hosts must have more than 350MB of free space in the /boot partition to support the Update Manager upgrade process. If the host that you are upgrading does not have more than 350MB of free space in the /boot partition, use a scripted or interactive upgrade instead.

Important After you upgrade or migrate your host to ESXi 5.x, you cannot roll back to your version 4.x ESX or ESXi software. Back up your host before you perform an upgrade or migration, so that, if the upgrade or migration fails, you can restore your 4.x host.

The wizard workflows prevent erroneous upgrade sequences. For example, the wizard prevents you from upgrading virtual machine hardware before you upgrade hosts in a cluster.

You can use Distributed Resource Scheduler (DRS) to prevent virtual machine downtime during the upgrade process.

Update Manager monitors hosts and virtual machines for compliance against your defined upgrade baselines. Noncompliance appears in detailed reports and in the dashboard view. Update Manager supports mass remediation.

The following vSphere components are upgraded by Update Manager.

- ESX and ESXi kernel (vmkernel)
- Virtual machine hardware
- VMware Tools
- Virtual appliances

For components that are not listed here, you can perform the upgrade by using another upgrade method, or, for third-party components, by using the appropriate third-party tools.

The following topics describe how to use Update Manager to conduct an orchestrated upgrade of your ESXi hosts.

- "Configuring Host and Cluster Settings," on page 167
- "Perform an Orchestrated Upgrade of Hosts Using vSphere Update Manager," on page 168

To use Update Manager to conduct an orchestrated upgrade of virtual machines on your hosts, see the *Installing and Administering VMware vSphere Update Manager* documentation.

Configuring Host and Cluster Settings

When you update vSphere objects in a cluster with DRS, VMware High Availability (HA), and VMware Fault Tolerance (FT) enabled, you can choose to temporarily disable VMware Distributed Power Management (DPM), HA admission control, and FT for the entire cluster. When the update completes, Update Manager restores these features.

Updates might require that the host enters maintenance mode during remediation. Virtual machines cannot run when a host is in maintenance mode. To ensure availability, vCenter Server can migrate virtual machines to other ESX/ESXi hosts within a cluster before the host is put into maintenance mode. vCenter Server migrates the virtual machines if the cluster is configured for vMotion, and if DRS is enabled.

If a host has no running virtual machines, VMware DPM might put the host in standby mode and interrupt an Update Manager operation. To make sure that scanning and staging complete successfully, Update Manager disables VMware DPM during these operations. To ensure successful remediation, you should allow Update Manager to disable VMware DPM and HA admission control before the remediation operation. After the operation completes, Update Manager restores VMware DPM and HA admission control. Update Manager disables HA admission control before staging and remediation but not before scanning.

If VMware DPM has already put hosts in standby mode, Update Manager powers on the hosts before scanning, staging, and remediation. After the scanning, staging, or remediation is complete, Update Manager turns on VMware DPM and HA admission control and lets VMware DPM put hosts into standby mode, if needed. Update Manager does not remediate powered off hosts.

If hosts are put into standby mode and VMware DPM is manually disabled for a reason, Update Manager does not remediate or power on the hosts.

Within a cluster, you should select to temporarily disable HA admission control to allow vMotion to proceed, in order to prevent downtime of the machines on the hosts you remediate. After the remediation of the entire cluster, Update Manager restores HA admission control settings.

If FT is turned on for any of the virtual machines on hosts within a cluster, you should select to temporarily turn off FT before performing any Update Manager operations on the cluster. If FT is turned on for any of the virtual machines on a host, Update Manager does not remediate that host. You should remediate all hosts in a cluster with the same updates, so that FT can be re-enabled after the remediation, because a primary virtual machine and a secondary virtual machine cannot reside on hosts of different ESX/ESXi version and patch level.

There are some specifics about remediating hosts that are part of a Virtual SAN cluster:

- The host remediation process might take extensive amount of time to complete.
- By design only one host from a Virtual SAN cluster can be in a maintenance mode at any time.
- Update Manager remediates hosts that are part of a Virtual SAN cluster sequentially even if you select the option to remediate them in parallel.

- If a host is a member of a Virtual SAN cluster, and any virtual machine on the host uses a VM storage policy with a setting for "Number of failures to tolerate=0", the host might experience unusual delays when entering maintenance mode. The delay occurs because Virtual SAN has to migrate the virtual machine data from one disk to another in the Virtual SAN datastore cluster. Delays might take up to hours. You can workaround this by setting the "Number of failures to tolerate=1" for the VM storage policy, which results in creating two copies of the virtual machine files in the Virtual SAN datastore.

Perform an Orchestrated Upgrade of Hosts Using vSphere Update Manager

You can use Update Manager to perform orchestrated upgrades of the ESX/ESXi hosts in your vSphere inventory by using a single upgrade baseline, or by using a baseline group.

This workflow describes the overall process to perform an orchestrated upgrade of the hosts in your vSphere inventory. Update Manager 5.x supports host upgrades to ESXi 5.x for hosts that are running ESX/ESXi 4.x.

You can perform orchestrated upgrades of hosts at the folder, cluster, or datacenter level.

NOTE The last two steps in this procedure are alternatives. Choose one or the other.

Prerequisites

- Make sure your system meets the requirements for vCenter Server 5.x, ESXi 5.x, and Update Manager 5.x. See "Update Manager Hardware Requirements," on page 28
- Install or upgrade vCenter Server to version 5.x. See Chapter 4, "Upgrading vCenter Server," on page 61.
- Install or upgrade vSphere Update Manager to version 5.x. See Chapter 6, "Upgrading Update Manager," on page 139.

Procedure

1 Configure Host Maintenance Mode Settings on page 169

ESX/ESXi host updates might require that the host enters maintenance mode before they can be applied. Update Manager puts the ESX/ESXi hosts in maintenance mode before applying these updates. You can configure how Update Manager responds if the host fails to enter maintenance mode.

2 Configure Cluster Settings on page 170

For ESX/ESXi hosts in a cluster, the remediation process can run either in a sequence or in parallel. Certain features might cause remediation failure. If you have VMware DPM, HA admission control, or Fault Tolerance enabled, you should temporarily disable these features to make sure that the remediation is successful.

3 Enable Remediation of PXE Booted ESXi 5.x Hosts on page 171

You can configure Update Manager to let other software initiate remediation of PXE booted ESXi 5.x hosts. The remediation installs patches and software modules on the hosts, but typically the host updates are lost after a reboot.

4 Import Host Upgrade Images and Create Host Upgrade Baselines on page 172

You can create upgrade baselines for ESX/ESXi hosts with ESXi 5.5 images that you import to the Update Manager repository.

5 Create a Host Baseline Group on page 173

You can combine one host upgrade baseline with multiple patch or extension baselines, or combine multiple patch and extension baselines in a baseline group.

6 Attach Baselines and Baseline Groups to Objects on page 174

To view compliance information and remediate objects in the inventory against specific baselines and baseline groups, you must first attach existing baselines and baseline groups to these objects.

7 Manually Initiate a Scan of ESX/ESXi Hosts on page 174

Before remediation, you should scan the vSphere objects against the attached baselines and baseline groups. To run a scan of hosts in the vSphere inventory immediately, initiate a scan manually.

8 View Compliance Information for vSphere Objects on page 175

You can review compliance information for the virtual machines, virtual appliances, and hosts against baselines and baseline groups that you attach.

9 Remediate Hosts Against an Upgrade Baseline on page 175

You can remediate ESX/ESXi hosts against a single attached upgrade baseline at a time. You can upgrade or migrate all hosts in your vSphere inventory by using a single upgrade baseline containing an ESXi 5.5 image.

10 Remediate Hosts Against Baseline Groups on page 178

You can remediate hosts against attached groups of upgrade, patch, and extension baselines. Baseline groups might contain multiple patch and extension baselines, or an upgrade baseline combined with multiple patch and extension baselines.

Configure Host Maintenance Mode Settings

ESX/ESXi host updates might require that the host enters maintenance mode before they can be applied. Update Manager puts the ESX/ESXi hosts in maintenance mode before applying these updates. You can configure how Update Manager responds if the host fails to enter maintenance mode.

For hosts in a container different from a cluster or for individual hosts, migration of the virtual machines with vMotion cannot be performed. If vCenter Server cannot migrate the virtual machines to another host, you can configure how Update Manager responds.

Hosts that are part of a Virtual SAN cluster can enter maintenance mode only one at a time. This is specificity of the Virtual SAN clusters.

If a host is a member of a Virtual SAN cluster, and any virtual machine on the host uses a VM storage policy with a setting for "Number of failures to tolerate=0", the host might experience unusual delays when entering maintenance mode. The delay occurs because Virtual SAN has to migrate the virtual machine data from one disk to another in the Virtual SAN datastore cluster. Delays might take up to hours. You can workaround this by setting the "Number of failures to tolerate=1" for the VM storage policy, which results in creating two copies of the virtual machine files in the Virtual SAN datastore.

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and on the Home page, click **Update Manager** under Solutions and Applications. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

1 On the **Configuration** tab, under Settings, click **ESX Host/Cluster Settings**.

2 Under Maintenance Mode Settings, select an option from the **VM Power state** drop-down menu to determine the change of the power state of the virtual machines and appliances that are running on the host to be remediated.

Option	Description
Power Off virtual machines	Powers off all virtual machines and virtual appliances before remediation.
Suspend virtual machines	Suspends all running virtual machines and virtual appliances before remediation.
Do Not Change VM Power State	Leaves virtual machines and virtual appliances in their current power state. This is the default setting.

3 (Optional) Select **Retry entering maintenance mode in case of failure**, specify the retry delay, and the number of retries.

If a host fails to enter maintenance mode before remediation, Update Manager waits for the retry delay period and retries putting the host into maintenance mode as many times as you indicate in **Number of retries** field.

4 (Optional) Select **Temporarily disable any removable media devices that might prevent a host from entering maintenance mode**.

Update Manager does not remediate hosts on which virtual machines have connected CD/DVD or floppy drives. All removable media drives that are connected to the virtual machines on a host might prevent the host from entering maintenance mode and interrupt remediation.

After remediation, Update Manager reconnects the removable media devices if they are still available.

5 Click **Apply**.

These settings become the default failure response settings. You can specify different settings when you configure individual remediation tasks.

Configure Cluster Settings

For ESX/ESXi hosts in a cluster, the remediation process can run either in a sequence or in parallel. Certain features might cause remediation failure. If you have VMware DPM, HA admission control, or Fault Tolerance enabled, you should temporarily disable these features to make sure that the remediation is successful.

NOTE Remediating hosts in parallel can improve performance significantly by reducing the time required for cluster remediation. Update Manager remediates hosts in parallel without disrupting the cluster resource constraints set by DRS. Avoid remediating hosts in parallel if the hosts are part of a Virtual SAN cluster. Due to the specifics of the Virtual SAN cluster, a host cannot enter maintenance mode while other hosts in the cluster are currently in maintenance mode.

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and on the Home page, click **Update Manager** under Solutions and Applications. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

1 On the **Configuration** tab, under Settings, click **ESX Host/Cluster Settings**.

2 Select the check boxes for features that you want to disable or enable.

Option	Description
Distributed Power Management (DPM)	VMware DPM monitors the resource use of the running virtual machines in the cluster. If sufficient excess capacity exists, VMware DPM recommends moving virtual machines to other hosts in the cluster and placing the original host into standby mode to conserve power. If the capacity is insufficient, VMware DPM might recommend returning standby hosts to a powered-on state. If you do not choose to disable DPM, Update Manager skips the cluster on which VMware DPM is enabled. If you choose to temporarily disable VMware DPM, Update Manager disables DPM on the cluster, remediates the hosts in the cluster, and re-enables VMware DPM after remediation is complete.
High Availability (HA) admission control	Admission control is a policy used by VMware HA to ensure failover capacity within a cluster. If HA admission control is enabled during remediation, the virtual machines within a cluster might not migrate with vMotion. If you do not choose to disable HA admission control, Update Manager skips the cluster on which HA admission control is enabled. If you choose to temporarily disable HA admission control, Update Manager disables HA admission control, remediates the cluster, and re-enables HA admission control after remediation is complete.
Fault Tolerance (FT)	FT provides continuous availability for virtual machines by automatically creating and maintaining a secondary virtual machine that is identical to the primary virtual machine. If you do not choose to turn off FT for the virtual machines on a host, Update Manager does not remediate that host.
Enable parallel remediation for hosts in cluster	Update Manager can remediate hosts in clusters in a parallel manner. Update Manager continuously evaluates the maximum number of hosts it can remediate in parallel without disrupting DRS settings. If you do not select the option, Update Manager remediates the hosts in a cluster sequentially. By design only one host from a Virtual SAN cluster can be in a maintenance mode at any time. Update Manager remediates hosts that are part of a Virtual SAN cluster sequentially even if you select the option to remediate them in parallel.
Migrate powered off and suspended virtual machines to other hosts in the cluster, if a host must enter maintenance mode	Update Manager migrates the suspended and powered off virtual machines from hosts that must enter maintenance mode to other hosts in the cluster. You can select to power off or suspend virtual machines before remediation in the Maintenance Mode Settings pane.

3 Click **Apply**.

These settings become the default failure response settings. You can specify different settings when you configure individual remediation tasks.

Enable Remediation of PXE Booted ESXi 5.x Hosts

You can configure Update Manager to let other software initiate remediation of PXE booted ESXi 5.x hosts. The remediation installs patches and software modules on the hosts, but typically the host updates are lost after a reboot.

The global setting in the Update Manager **Configuration** tab enables solutions such as ESX Agent Manager or Cisco Nexus 1000V to initiate remediation of PXE booted ESXi 5.x hosts. In contrast, the **Enable patch remediation of powered on PXE booted ESXi hosts** setting in the Remediate wizard enables Update Manager to patch PXE booted hosts.

To retain updates on stateless hosts after a reboot, use a PXE boot image that contains the updates. You can update the PXE boot image before applying the updates with Update Manager, so that the updates are not lost because of a reboot. Update Manager itself does not reboot the hosts because it does not install updates requiring a reboot on PXE booted ESXi 5.x hosts.

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and on the Home page, click **Update Manager** under Solutions and Applications. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

1 On the **Configuration** tab, under Settings, click **ESX Host/Cluster Settings**.

2 To enable installation of software for solutions on PXE booted ESXi 5.x hosts, select **Allow installation of additional software on PXE booted ESXi 5.x hosts.**

3 Click **Apply**.

Import Host Upgrade Images and Create Host Upgrade Baselines

You can create upgrade baselines for ESX/ESXi hosts with ESXi 5.5 images that you import to the Update Manager repository.

You can use ESXi `.iso` images to upgrade ESXi 4.x, ESXi 5.0 and ESXi 5.1 hosts to ESXi 5.5 or migrate ESX 4.x hosts to ESXi 5.5.

To upgrade or migrate hosts, use the ESXi installer image distributed by VMware with the name format `VMware-VMvisor-Installer-5.5.0-`*`build_number`*`.x86_64.iso` or a custom image created by using Image Builder.

Prerequisites

Ensure that you have the **Upload File** privilege. For more information about managing users, groups, roles, and permissions, see *vCenter Server and Host Management*.

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and on the Home page, click **Update Manager** under Solutions and Applications. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

1 On the **ESXi Images** tab click **Import ESXi Image** on the upper-right side.

2 On the Select ESXi Image page of the Import ESXi Image wizard, browse to and select the ESXi image that you want to upload.

3 Click **Next**.

CAUTION Do not close the import wizard. Closing the import wizard stops the upload process.

4 (Optional) In the Security Warning window, select an option to handle the certificate warning.

A trusted certificate authority does not sign the certificates that are generated for vCenter Server and ESX/ESXi hosts during installation. Because of this, each time an SSL connection is made to one of these systems, the client displays a warning.

Option	Action
Ignore	Click **Ignore** to continue using the current SSL certificate and start the upload process.
Cancel	Click **Cancel** to close the window and stop the upload process.
Install this certificate and do not display any security warnings	Select this check box and click **Ignore** to install the certificate and stop receiving security warnings.

5 After the file is uploaded, click **Next**.

6 (Optional) Create a host upgrade baseline.

   a Leave the **Create a baseline using the ESXi image** selected.

   b Specify a name, and optionally, a description for the host upgrade baseline.

7 Click **Finish**.

The ESXi image that you uploaded appears in the Imported ESXi Images pane. You can see more information about the software packages that are included in the ESXi image in the Software Packages pane.

If you also created a host upgrade baseline, the new baseline is displayed in the Baselines pane of the **Baselines and Groups** tab.

What to do next

To upgrade or migrate the hosts in your environment, you must create a host upgrade baseline if you have not already done so.

Create a Host Baseline Group

You can combine one host upgrade baseline with multiple patch or extension baselines, or combine multiple patch and extension baselines in a baseline group.

NOTE You can click **Finish** in the New Baseline Group wizard at any time to save your baseline group and add baselines to it at a later stage.

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and on the Home page, click **Update Manager** under Solutions and Applications. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

1 On the **Baselines and Groups** tab, click **Create** above the Baseline Groups pane.

2 Enter a unique name for the baseline group.

3 Under Baseline Group Type, select **Host Baseline Group** and click **Next**.

4 Select a host upgrade baseline to include it in the baseline group.

5 (Optional) Create a new host upgrade baseline by clicking **Create a new Host Upgrade Baseline** at the bottom of the Upgrades page and complete the New Baseline wizard.

6 Click **Next**.

7 Select the patch baselines that you want to include in the baseline group.

8 (Optional) Create a new patch baseline by clicking **Create a new Host Patch Baseline** at the bottom of the Patches page and complete the New Baseline wizard.

9 Click **Next**.

10 Select the extension baselines to include in the baseline group.

11 (Optional) Create a new extension baseline by clicking **Create a new Extension Baseline** at the bottom of the Patches page and complete the New Baseline wizard.

12 On the Ready to Complete page, click **Finish**.

The host baseline group is displayed in the Baseline Groups pane.

Attach Baselines and Baseline Groups to Objects

To view compliance information and remediate objects in the inventory against specific baselines and baseline groups, you must first attach existing baselines and baseline groups to these objects.

You can attach baselines and baseline groups to objects from the Update Manager Client Compliance view.

Although you can attach baselines and baseline groups to individual objects, a more efficient method is to attach them to container objects, such as folders, vApps, clusters, and datacenters. Individual vSphere objects inherit baselines attached to the parent container object. Removing an object from a container removes the inherited baselines from the object.

If your vCenter Server system is part of a connected group in vCenter Linked Mode, you can attach baselines and baseline groups to objects managed by the vCenter Server system with which Update Manager is registered. Baselines and baseline groups you attach are specific for the Update Manager instance that is registered with the vCenter Server system.

Prerequisites

Ensure that you have the **Attach Baseline** privilege.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered and select **Home > Inventory** in the navigation bar.

2 Select the type of object that you want to attach the baseline to.

For example, **Hosts and Clusters** or **VMs and Templates**.

3 Select the object in the inventory, and click the **Update Manager** tab.

If your vCenter Server system is part of a connected group in vCenter Linked Mode, the **Update Manager** tab is available only for the vCenter Server system with which an Update Manager instance is registered.

4 Click **Attach** in the upper-right corner.

5 In the Attach Baseline or Group window, select one or more baselines or baseline groups to attach to the object.

If you select one or more baseline groups, all baselines in the groups are selected. You cannot deselect individual baselines in a group.

6 (Optional) Click the **Create Baseline Group** or **Create Baseline** links to create a baseline group or a baseline and complete the remaining steps in the respective wizard.

7 Click **Attach**.

The baselines and baseline groups that you selected to attach are displayed in the Attached Baseline Groups and Attached Baselines panes of the **Update Manager** tab.

Manually Initiate a Scan of ESX/ESXi Hosts

Before remediation, you should scan the vSphere objects against the attached baselines and baseline groups. To run a scan of hosts in the vSphere inventory immediately, initiate a scan manually.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered and select **Home > Inventory > Hosts and Clusters** in the navigation bar.

2 Right-click a host, datacenter, or any container object and select **Scan for Updates**.

3 Select the types of updates to scan for.

You can scan for either **Patches and Extensions** or **Upgrades**.

4 Click **Scan**.

The selected inventory object and all child objects are scanned against all patches, extensions, and upgrades in the attached baselines. The larger the virtual infrastructure and the higher up in the object hierarchy that you initiate the scan, the longer the scan takes.

View Compliance Information for vSphere Objects

You can review compliance information for the virtual machines, virtual appliances, and hosts against baselines and baseline groups that you attach.

When you select a container object, you view the overall compliance status of the attached baselines, as well as all the individual compliance statuses. If you select an individual baseline attached to the container object, you see the compliance status of the baseline.

If you select an individual virtual machine, appliance, or host, you see the overall compliance status of the selected object against all attached baselines and the number of updates. If you further select an individual baseline attached to this object, you see the number of updates grouped by the compliance status for that baseline.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered and select **Home > Inventory** in the navigation bar.

2 Select the type of object for which you want to view compliance information.

For example, **Hosts and Clusters** or **VMs and Templates**.

3 Select an object from the inventory.

4 Click the **Update Manager** tab to view the scan results and compliance states.

Remediate Hosts Against an Upgrade Baseline

You can remediate ESX/ESXi hosts against a single attached upgrade baseline at a time. You can upgrade or migrate all hosts in your vSphere inventory by using a single upgrade baseline containing an ESXi 5.5 image.

NOTE Alternatively, you can upgrade hosts by using a baseline group. See "Remediate Hosts Against Baseline Groups," on page 178.

Update Manager 5.5 supports upgrade from ESXi 4.x, ESXi 5.0 and ESXi 5.1 to ESXi 5.5 and migration from ESX 4.x to ESXi 5.5. You cannot use Update Manager to upgrade a host to ESXi 5.5 if the host was upgraded from ESX 3.x to ESX 4.x. Such hosts do not have sufficient free space in the `/boot` partition to support the Update Manager upgrade process. Use a scripted or interactive upgrade instead.

To upgrade or migrate hosts, use the ESXi installer image distributed by VMware with the name format `VMware-VMvisor-Installer-5.5.0-build_number.x86_64.iso` or a custom image created by using Image Builder.

NOTE In case of an unsuccessful upgrade or migration from ESX/ESXi 4.x, ESXi 5.0 or ESXi 5.1 to ESXi 5.5, you cannot roll back to your previous ESX/ESXi 4.x, ESXi 5.0 or ESXi 5.1 instance.

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered. If your vCenter Server system is a part of a connected group in vCenter Linked Mode, specify the Update Manager instance by selecting the name of the corresponding vCenter Server system in the navigation bar.

To remediate a host against an upgrade baseline, attach the baseline to the host.

Review any scan messages in the Upgrade Details window for potential problems with hardware, third-party software, and configuration issues that might prevent a successful upgrade or migration to ESXi 5.5.

Procedure

1 On the **Home** page of the vSphere Client, select **Hosts and Clusters** and click the **Update Manager** tab.

2 Right-click the inventory object you want to remediate and select **Remediate**.

If you select a container object, all hosts under the selected object are remediated.

3 On the Remediation Selection page of the Remediate wizard, select the upgrade baseline to apply.

4 (Optional) Select the hosts that you want to remediate and click **Next**.

If you have chosen to remediate a single host and not a container object, the host is selected by default.

5 On the End User License Agreement page, accept the terms and click **Next**.

6 (Optional) On the ESXi 5.5 Upgrade page, select the option to remove any installed third-party software modules that are incompatible with the upgrade and ignore warnings about unsupported devices on the host in order to continue with the remediation.

In case any additional third-party modules installed on the hosts are incompatible with the upgrade, the upgrade remediation does not succeed. To proceed and upgrade to ESXi 5.5 your ESX/ESXi hosts that contain third-party modules by using an ESXi image without the corresponding VIBs, you must choose to remove the third-party software on the hosts.

NOTE ESXi 5.0, ESXi 5.1 and ESXi 5.5 hosts are binary compatible. Any hardware or third-party software modules on a ESXi 5.0 or a ESXi 5.1 host will remain intact after upgrade to ESXi 5.5.

7 Click **Next**.

8 On the Schedule page, specify a unique name and an optional description for the task.

9 Select **Immediately** to begin the process immediately after you complete the wizard, or specify a time for the remediation process to begin, and click **Next**.

10 On the Host Remediation Options page, from the **Power state** drop-down menu, you can select the change in the power state of the virtual machines and virtual appliances that are running on the hosts to be remediated.

Option	Description
Power Off virtual machines	Power off all virtual machines and virtual appliances before remediation.
Suspend virtual machines	Suspend all running virtual machines and virtual appliances before remediation.
Do Not Change VM Power State	Leave virtual machines and virtual appliances in their current power state. A host cannot enter maintenance mode until virtual machines on the host are powered off, suspended, or migrated with vMotion to other hosts in a DRS cluster.

Some updates require that a host enters maintenance mode before remediation. Virtual machines and appliances cannot run when a host is in maintenance mode.

To reduce the host remediation downtime at the expense of virtual machine availability, you can choose to shut down or suspend virtual machines and virtual appliances before remediation. In a DRS cluster, if you do not power off the virtual machines, the remediation takes longer but the virtual machines are available during the entire remediation process, because they are migrated with vMotion to other hosts.

11 (Optional) Select **Retry entering maintenance mode in case of failure**, specify the number of retries, and specify the time to wait between retries.

Update Manager waits for the retry delay period and retries putting the host into maintenance mode as many times as you indicate in **Number of retries** field.

12 (Optional) Select **Disable any removable media devices connected to the virtual machine on the host**.

Update Manager does not remediate hosts on which virtual machines have connected CD, DVD, or floppy drives. In cluster environments, connected media devices might prevent vMotion if the destination host does not have an identical device or mounted ISO image, which in turn prevents the source host from entering maintenance mode.

After remediation, Update Manager reconnects the removable media devices if they are still available.

13 Click **Next**.

14 Edit the cluster remediation options.

The Cluster Remediation Options page is available only when you remediate hosts in a cluster.

Option	Details
Disable Distributed Power Management (DPM) if it is enabled for any of the selected clusters.	Update Manager does not remediate clusters with active DPM. DPM monitors the resource use of the running virtual machines in the cluster. If sufficient excess capacity exists, DPM recommends moving virtual machines to other hosts in the cluster and placing the original host into standby mode to conserve power. Putting hosts into standby mode might interrupt remediation.
Disable High Availability admission control if it is enabled for any of the selected clusters.	Update Manager does not remediate clusters with active HA admission control. Admission control is a policy used by VMware HA to ensure failover capacity within a cluster. If HA admission control is enabled during remediation, the virtual machines within a cluster might not migrate with vMotion.
Disable Fault Tolerance (FT) if it is enabled for the VMs on the selected hosts.	If FT is turned on for any of the virtual machines on a host, Update Manager does not remediate that host. For FT to be enabled, the hosts on which the Primary and Secondary virtual machines run must be of the same version and must have the same patches installed. If you apply different patches to these hosts, FT cannot be re-enabled.
Enable parallel remediation for the hosts in the selected clusters.	Remediate hosts in clusters in a parallel manner. If the setting is not selected, Update Manager remediates the hosts in a cluster sequentially. By design only one host from a Virtual SAN cluster can be in a maintenance mode at any time. Update Manager remediates hosts that are part of a Virtual SAN cluster sequentially even if you select the option to remediate them in parallel. By default, Update Manager continuously evaluates the maximum number of hosts it can remediate concurrently without disrupting DRS settings. You can limit the number of concurrently remediated hosts to a specific number. **NOTE** Update Manager remediates concurrently only the hosts on which virtual machines are powered off or suspended. You can choose to power off or suspend virtual machines from the **Power State** menu in the Maintenance Mode Settings pane on the Host Remediation Options page.
Migrate powered off and suspended virtual machines to other hosts in the cluster, if a host must enter maintenance mode.	Update Manager migrates the suspended and powered off virtual machines from hosts that must enter maintenance mode to other hosts in the cluster. You can choose to power off or suspend virtual machines before remediation in the Maintenance Mode Settings pane.

15 (Optional) Generate a cluster remediation options report by clicking **Generate Report** on the Cluster Remediation Options page and click **Next**.

16 On the Ready to Complete page, click **Finish**.

NOTE In the Recent Tasks pane, the remediation task is displayed and will remain at about 22 percent for most of the process. The process is still running and will take approximately 15 minutes to complete.

Remediate Hosts Against Baseline Groups

You can remediate hosts against attached groups of upgrade, patch, and extension baselines. Baseline groups might contain multiple patch and extension baselines, or an upgrade baseline combined with multiple patch and extension baselines.

You can perform an orchestrated upgrade by using a host baseline group. The upgrade baseline in the baseline group runs first, followed by patch and extension baselines.

NOTE Alternatively, you can upgrade hosts by using a single upgrade baseline. See "Remediate Hosts Against an Upgrade Baseline," on page 175.

Prerequisites

Ensure that at least one baseline group is attached to the host.

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered. If your vCenter Server system is a part of a connected group in vCenter Linked Mode, specify the Update Manager instance by selecting the name of the corresponding vCenter Server system in the navigation bar.

Review any scan messages in the Upgrade Details window for potential problems with hardware, third-party software, and configuration issues that might prevent a successful upgrade or migration to ESXi 5.0.

Procedure

1 On the **Home** page of the vSphere Client, select **Hosts and Clusters** and click the **Update Manager** tab.

2 Right-click the inventory object you want to remediate and select **Remediate**.

If you select a container object, all hosts under the selected object are remediated.

3 On the Remediation Selection page of the Remediate wizard, select the baseline group and baselines to apply.

4 (Optional) Select the hosts that you want to remediate and click **Next**.

If you have chosen to remediate a single host and not a container object, the host is selected by default.

5 On the End User License Agreement page, accept the terms and click **Next**.

6 (Optional) On the ESXi 5.5 Upgrade page, select the option to remove any installed third-party software modules that are incompatible with the upgrade and ignore warnings about unsupported devices on the host in order to continue with the remediation.

In case any additional third-party modules installed on the hosts are incompatible with the upgrade, the upgrade remediation does not succeed. To proceed and upgrade to ESXi 5.5 your ESX/ESXi hosts that contain third-party modules by using an ESXi image without the corresponding VIBs, you must choose to remove the third-party software on the hosts.

NOTE ESXi 5.0, ESXi 5.1 and ESXi 5.5 hosts are binary compatible. Any hardware or third-party software modules on a ESXi 5.0 or a ESXi 5.1 host will remain intact after upgrade to ESXi 5.5.

7 Click **Next**.

8 (Optional) On the Patches and Extensions page, deselect specific patches or extensions to exclude them from the remediation process, and click **Next**.

9 (Optional) On the Dynamic Patches and Extensions to Exclude page, review the list of patches or extensions to be excluded and click **Next**.

10 On the Schedule page, specify a unique name and an optional description for the task.

11 Select **Immediately** to begin the process immediately after you complete the wizard, or specify a time for the remediation process to begin, and click **Next**.

12 On the Host Remediation Options page, from the **Power state** drop-down menu, you can select the change in the power state of the virtual machines and virtual appliances that are running on the hosts to be remediated.

Option	Description
Power Off virtual machines	Power off all virtual machines and virtual appliances before remediation.
Suspend virtual machines	Suspend all running virtual machines and virtual appliances before remediation.
Do Not Change VM Power State	Leave virtual machines and virtual appliances in their current power state. A host cannot enter maintenance mode until virtual machines on the host are powered off, suspended, or migrated with vMotion to other hosts in a DRS cluster.

Some updates require that a host enters maintenance mode before remediation. Virtual machines and appliances cannot run when a host is in maintenance mode.

To reduce the host remediation downtime at the expense of virtual machine availability, you can choose to shut down or suspend virtual machines and virtual appliances before remediation. In a DRS cluster, if you do not power off the virtual machines, the remediation takes longer but the virtual machines are available during the entire remediation process, because they are migrated with vMotion to other hosts.

13 (Optional) Select **Retry entering maintenance mode in case of failure**, specify the number of retries, and specify the time to wait between retries.

Update Manager waits for the retry delay period and retries putting the host into maintenance mode as many times as you indicate in **Number of retries** field.

14 (Optional) Select **Disable any removable media devices connected to the virtual machine on the host**.

Update Manager does not remediate hosts on which virtual machines have connected CD, DVD, or floppy drives. In cluster environments, connected media devices might prevent vMotion if the destination host does not have an identical device or mounted ISO image, which in turn prevents the source host from entering maintenance mode.

After remediation, Update Manager reconnects the removable media devices if they are still available.

15 (Optional) Select the check box under ESXi 5.x Patch Settings to enable Update Manager to patch powered on PXE booted ESXi hosts.

This option appears only when you remediate hosts against patch or extension baselines.

16 Click **Next**.

17 Edit the cluster remediation options.

The Cluster Remediation Options page is available only when you remediate hosts in a cluster.

Option	Details
Disable Distributed Power Management (DPM) if it is enabled for any of the selected clusters.	Update Manager does not remediate clusters with active DPM. DPM monitors the resource use of the running virtual machines in the cluster. If sufficient excess capacity exists, DPM recommends moving virtual machines to other hosts in the cluster and placing the original host into standby mode to conserve power. Putting hosts into standby mode might interrupt remediation.
Disable High Availability admission control if it is enabled for any of the selected clusters.	Update Manager does not remediate clusters with active HA admission control. Admission control is a policy used by VMware HA to ensure failover capacity within a cluster. If HA admission control is enabled during remediation, the virtual machines within a cluster might not migrate with vMotion.
Disable Fault Tolerance (FT) if it is enabled for the VMs on the selected hosts.	If FT is turned on for any of the virtual machines on a host, Update Manager does not remediate that host. For FT to be enabled, the hosts on which the Primary and Secondary virtual machines run must be of the same version and must have the same patches installed. If you apply different patches to these hosts, FT cannot be re-enabled.
Enable parallel remediation for the hosts in the selected clusters.	Remediate hosts in clusters in a parallel manner. If the setting is not selected, Update Manager remediates the hosts in a cluster sequentially. By design only one host from a Virtual SAN cluster can be in a maintenance mode at any time. Update Manager remediates hosts that are part of a Virtual SAN cluster sequentially even if you select the option to remediate them in parallel. By default, Update Manager continuously evaluates the maximum number of hosts it can remediate concurrently without disrupting DRS settings. You can limit the number of concurrently remediated hosts to a specific number. **Note** Update Manager remediates concurrently only the hosts on which virtual machines are powered off or suspended. You can choose to power off or suspend virtual machines from the **Power State** menu in the Maintenance Mode Settings pane on the Host Remediation Options page.
Migrate powered off and suspended virtual machines to other hosts in the cluster, if a host must enter maintenance mode.	Update Manager migrates the suspended and powered off virtual machines from hosts that must enter maintenance mode to other hosts in the cluster. You can choose to power off or suspend virtual machines before remediation in the Maintenance Mode Settings pane.

18 (Optional) Generate a cluster remediation options report by clicking **Generate Report** on the Cluster Remediation Options page and click **Next**.

19 On the Ready to Complete page, click **Finish**.

Note In the Recent Tasks pane, the remediation task is displayed and will remain at about 22 percent for most of the process. The process is still running and will take approximately 15 minutes to complete.

Upgrade or Migrate Hosts Interactively

You can boot the ESXi installer from a CD, DVD, or USB flash drive to upgrade ESX/ESXi 4.x, ESXi 5.0.x, and 5.1.x hosts to ESXi 5.5.

Important If you are performing a fresh ESXi installation, see the *vSphere Installation and Setup* documentation. The instructions in this *vSphere Upgrade* documentation are for an upgrade or migration of ESXi or ESX.

Before upgrading, consider disconnecting your network storage. This action decreases the time it takes the installer to search for available disk drives. When you disconnect network storage, any files on the disconnected disks are unavailable at installation. Do not disconnect a LUN that contains an existing ESX or ESXi installation. Do not disconnect a VMFS datastore that contains the Service Console of an existing ESX installation. These actions can affect the outcome of the installation.

IMPORTANT After you upgrade or migrate your host to ESXi 5.x, you cannot roll back to your version 4.x ESX or ESXi software. Back up your host before you perform an upgrade or migration, so that, if the upgrade or migration fails, you can restore your 4.x host.

Prerequisites

- You must have the ESXi installer ISO in one of the following locations.
  - On CD or DVD. If you do not have the installation CD/DVD, you can create one. See "Download and Burn the ESXi Installer ISO Image to a CD or DVD," on page 154
  - On a USB flash drive. See "Format a USB Flash Drive to Boot the ESXi Installation or Upgrade," on page 155

  NOTE You can also PXE boot the ESXi installer to launch an interactive installation or a scripted installation. See "PXE Booting the ESXi Installer," on page 158.
- Verify that the server hardware clock is set to UTC. This setting is in the system BIOS.
- ESXi Embedded must not be on the host. ESXi Installable and ESXi Embedded cannot exist on the same host.

Procedure

1. Insert the ESXi installer CD/DVD into the CD/DVD-ROM drive, or attach the Installer USB flash drive and restart the machine.
2. Set the BIOS to boot from the CD-ROM device or the USB flash drive.

   See your hardware vendor documentation for information on changing boot order.
3. In the Select a Disk panel, select the drive on which to install or upgrade ESXi and press **Enter**.

   Press F1 for information about the selected disk.

   NOTE Do not rely on the disk order in the list to select a disk. The disk order is determined by the BIOS. On systems where drives are continuously being added and removed, they might be out of order.
4. If the installer finds an existing ESX or ESXi installation and VMFS datastore you can choose from the following options:
   - **Upgrade ESXi, preserve VMFS datastore**
   - **Install ESXi, preserve VMFS datastore**
   - **Install ESXi, overwrite VMFS datastore**

   If an existing VMFS datastore cannot be preserved, you can choose only to install ESXi and overwrite the existing VMFS datastore, or to cancel the installation. If you choose to overwrite the existing VMFS datastore, back up the datastore first.

If you are migrating a 4.x host that contains custom VIBs that are not included in the ESXi installer ISO, the option **Upgrade ESXi, preserve VMFS datastore** is replaced with **Force Migrate ESXi, preserve VMFS datastore**.

CAUTION Using the Force Migrate option might cause the upgraded host to not boot properly, to exhibit system instability, or to lose functionality. If you are upgrading a 5.0.x or 5.1.x host, supported custom VIBs that are not included in the ESXi installer ISO are migrated. You do not need to to select the Force Migrate option. See "Upgrading Hosts That Have Third-Party Custom VIBs," on page 151.

5 Press F11 to confirm and start the upgrade.

6 When the upgrade is complete, remove the installation CD/DVD or USB flash drive.

7 Press Enter to reboot the host.

8 Set the first boot device to be the drive on which you upgraded ESXi in Step 3.

If an existing VMFS datastore cannot be preserved, you can choose only to install ESXi and overwrite the existing VMFS datastore, or to cancel the installation. If you choose to overwrite the existing VMFS datastore, back up the datastore first.

See your hardware vendor documentation for information on changing boot order.

Installing, Upgrading, or Migrating Hosts Using a Script

You can quickly deploy ESXi hosts using scripted, unattended installations or upgrades. Scripted installations, upgrades, or migrations provide an efficient way to deploy multiple hosts.

The installation or upgrade script contains the installation settings for ESXi. You can apply the script to all hosts that you want to have a similar configuration.

For a scripted installation, upgrade, or migration, you must use the supported commands to create a script. and edit the script to change settings that are unique for each host.

The installation or upgrade script can reside in one of the following locations:

- FTP
- HTTP/HTTPS
- NFS
- USB flash drive
- CDROM

Enter Boot Options to Start an Installation or Upgrade Script

You can start an installation or upgrade script by typing boot command-line options at the ESXi installer boot command line.

At boot time you might need to specify options to access the kickstart file. You can enter boot options by pressing Shift+O in the boot loader. For a PXE boot installation, you can pass options through the `kernelopts` line of the `boot.cfg` file. See "About the boot.cfg File," on page 193 and "PXE Booting the ESXi Installer," on page 158.

A `ks=...` option must be given, to specify the location of the installation script. Otherwise, a scripted installation or upgrade will not start. If `ks=...` is omitted, the text installer will proceed.

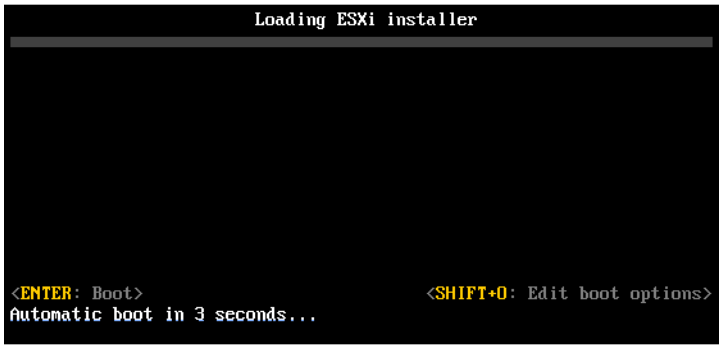
Supported boot options are listed in "Boot Options," on page 183.

IMPORTANT After you upgrade or migrate your host to ESXi 5.x, you cannot roll back to your version 4.x ESX or ESXi software. Back up your host before you perform an upgrade or migration, so that, if the upgrade or migration fails, you can restore your 4.x host.

Procedure

1 Start the host.

2 When the ESXi installer window appears, press Shift+O to edit boot options.



3 At the `runweasel` command prompt, type
`ks=`*`location of installation script plus boot command line options`*

Example: Boot Option

You type the following boot options:

```
ks=http://00.00.00.00/kickstart/ks-osdc-pdp101.cfg nameserver=00.00.0.0 ip=00.00.00.000
netmask=255.255.255.0 gateway=00.00.00.000
```

Boot Options

When you perform a scripted installation, you might need to specify options at boot time to access the kickstart file.

Supported Boot Options

Table 7-5. Boot Options for ESXi Installation

Boot Option	Description
`BOOTIF=`*`hwtype-MAC address`*	Similar to the `netdevice` option, except in the PXELINUX format as described in the IPAPPEND option under SYSLINUX at the syslinux.zytor.com site.
`gateway=`*`ip address`*	Sets this network gateway as the default gateway to be used for downloading the installation script and installation media.
`ip=`*`ip address`*	Sets up a static IP address to be used for downloading the installation script and the installation media. Note: the PXELINUX format for this option is also supported. See the IPAPPEND option under SYSLINUX at the syslinux.zytor.com site.
`ks=cdrom:/`*`path`*	Performs a scripted installation with the script at *path*, which resides on the CD in the CD-ROM drive. Each CDROM is mounted and checked until the file that matches the path is found.
`ks=file://`*`path`*	Performs a scripted installation with the script at *path*.
`ks=`*`protocol`*`://`*`serverpath`*	Performs a scripted installation with a script located on the network at the given URL. *protocol* can be `http`, `https`, `ftp`, or `nfs`. An example using nfs protocol is `ks=nfs://`*`host`*`:`*`porturl-path`*. The format of an NFS URL is specified in RFC 2224.

Table 7-5. Boot Options for ESXi Installation (Continued)

Boot Option	Description
`ks=usb`	Performs a scripted installation, accessing the script from an attached USB drive. Searches for a file named `ks.cfg`. The file must be located in the root directory of the drive. If multiple USB flash drives are attached, they are searched until the `ks.cfg` file is found. Only FAT16 and FAT32 file systems are supported.
`ks=usb:/path`	Performs a scripted installation with the script file at the specified path, which resides on USB.
`ksdevice=device`	Tries to use a network adapter *device* when looking for an installation script and installation media. Specify as a MAC address, for example, 00:50:56:C0:00:01. This location can also be a vmnicNN name. If not specified and files need to be retrieved over the network, the installer defaults to the first discovered network adapter that is plugged in.
`nameserver=ip address`	Specifies a domain name server to be used for downloading the installation script and installation media.
`netdevice=device`	Tries to use a network adapter *device* when looking for an installation script and installation media. Specify as a MAC address, for example, 00:50:56:C0:00:01. This location can also be a vmnicNN name. If not specified and files need to be retrieved over the network, the installer defaults to the first discovered network adapter that is plugged in.
`netmask=subnet mask`	Specifies subnet mask for the network interface that downloads the installation script and the installation media.
`vlanid=vlanid`	Configure the network card to be on the specified VLAN.

About Installation and Upgrade Scripts

The installation/upgrade script is a text file, for example `ks.cfg`, that contains supported commands.

The command section of the script contains the ESXi installation options. This section is required and must appear first in the script.

Locations Supported for Installation or Upgrade Scripts

In scripted installations and upgrades, the ESXi installer can access the installation or upgrade script, also called the kickstart file, from several locations.

The following locations are supported for the installation or upgrade script:

- CD/DVD. See "Create an Installer ISO Image with a Custom Installation or Upgrade Script," on page 157.
- USB Flash drive. See "Create a USB Flash Drive to Store the ESXi Installation Script or Upgrade Script," on page 156.
- A network location accessible through the following protocols: NFS, HTTP, HTTPS, FTP

Path to the Installation or Upgrade Script

You can specify the path to an installation or upgrade script.

`ks=http://XXX.XXX.XXX.XXX/kickstart/KS.CFG` is the path to the ESXi installation script, where *XXX.XXX.XXX.XXX* is the IP address of the machine where the script resides. See "About Installation and Upgrade Scripts," on page 184.

To start an installation script from an interactive installation, you enter the `ks=` option manually. See "Enter Boot Options to Start an Installation or Upgrade Script," on page 182.

Installation and Upgrade Script Commands

To modify the default installation or upgrade script or to create your own script, use supported commands. Use supported commands in the installation script, which you specify with a boot command when you boot the installer.

To determine which disk to install or upgrade ESXi on, the installation script requires one of the following commands: `install`, `upgrade`, or `installorupgrade`. The `install` command creates the default partitions, including a VMFS datastore that occupies all available space after the other partitions are created. The `install` command replaces the `autopart` command that was used for scripted ESXi 4.1 installations.

accepteula or vmaccepteula (required)

Accepts the ESXi license agreement. This command functions as it did in ESXi 4.1.

clearpart (optional)

Compared to kickstart, the behavior of the ESXi `clearpart` command is different. Carefully edit the `clearpart` command in your existing scripts.

Clears any existing partitions on the disk. Requires `install` command to be specified.

`--drives=`	Remove partitions on the specified drives.
`--alldrives`	Ignores the `--drives=` requirement and allows clearing of partitions on every drive.
`--ignoredrives=`	Removes partitions on all drives except those specified. Required unless the `--drives=` or `--alldrives` flag is specified.
`--overwritevmfs`	Permits overwriting of VMFS partitions on the specified drives. By default, overwriting VMFS partitions is not allowed.
`--firstdisk=` ***`disk-type1`*** **`[`*`disk-type2`*`,...]`**	Partitions the first eligible disk found. By default, the eligible disks are set to the following order: 1 Locally attached storage (`local`) 2 Network storage (`remote`) 3 USB disks (`usb`) You can change the order of the disks by using a comma separated list appended to the argument. If you provide a filter list, the default settings are overridden. You can combine filters to specify a particular disk, including `esx` for the first disk with ESX installed on it, model and vendor information, or the name of the vmkernel device driver. For example, to prefer a disk with the model name ST3120814A and any disk that uses the mptsas driver rather than a normal local disk, the argument is `--firstdisk=ST3120814A,mptsas,local`.

dryrun (optional)

Parses and checks the installation script. Does not perform the installation.

install

Specifies that this is a fresh installation. Replaces the deprecated `autopart` command used for ESXi 4.1 scripted installations. Either the `install`, `upgrade`, or `installorupgrade` command is required to determine which disk to install or upgrade ESXi on.

`--disk= or --drive=`

Specifies the disk to partition. In the command `--disk=`*`diskname`*, the *diskname* can be in any of the forms shown in the following examples:

- Path: `--disk=`*`/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0`*
- MPX name: `--disk=`*`mpx.vmhba1:C0:T0:L0`*
- VML name: `--disk=`*`vml.000000034211234`*
- vmkLUN UID: `--disk=`*`vmkLUN_UID`*

For accepted disk name formats, see "Disk Device Names," on page 193.

`--firstdisk=`
***`disk-type1`*`,`**
`[`*`disk-type2`*`,...]`

Partitions the first eligible disk found. By default, the eligible disks are set to the following order:

1 Locally attached storage (`local`)

2 Network storage (`remote`)

3 USB disks (`usb`)

You can change the order of the disks by using a comma separated list appended to the argument. If you provide a filter list, the default settings are overridden. You can combine filters to specify a particular disk, including `esx` for the first disk with ESX installed on it, model and vendor information, or the name of the vmkernel device driver. For example, to prefer a disk with the model name ST3120814A and any disk that uses the mptsas driver rather than a normal local disk, the argument is `--firstdisk=ST3120814A,mptsas,local`.

`--ignoressd`

Excludes solid-state disks (S`--firstdisk`SDs) from eligibility for partitioning. This option can be used with the `install` command and the `--firstdisk` option. This option takes precedence over the `--firstdisk` option. This option is invalid with the `--drive` or `--disk` options and with the `upgrade` and `installorupgrade` commands. See the *vSphere Storage* documentation for more information about preventing SSD formatting during auto-partitioning.

`--overwritevsan`

You must use the `--overwritevsan` option when you install ESXi on a disk, either SSD or HDD (magnetic), that is in a Virtual SAN disk group. If you use this option and there is no Virtual SAN partition on the selected disk, the installation will fail. When you install ESXi on a disk that is in Virtual SAN disk group, the result depends on the disk you select:

- If you select an SSD, the SSD and all underlying HDDs in the same disk group will be wiped.
- If you select an HDD, and the disk group size is greater than two, only the selected HDD will be wiped.
- If you select an HDD disk, and the disk group size is two or less, the SSD and the selected HDD will be wiped.

For more information about managing Virtual SAN disk groups, see the *vSphere Storage* documentation.

--overwritevmfs Required to overwrite an existing VMFS datastore on the disk before installation.

--preservevmfs Preserves an existing VMFS datastore on the disk during installation.

--novmfsondisk Prevents a VMFS partition from being created on this disk. Must be used with `--overwritevmfs` if a VMFS partition already exists on the disk.

installorupgrade

Either the `install`, `upgrade`, or `installorupgrade` command is required to determine which disk to install or upgrade ESXi on.

--disk= or --drive= Specifies the disk to partition. In the command `--disk=`*`diskname`*, the *diskname* can be in any of the forms shown in the following examples:

- Path: `--disk=`*`/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0`*
- MPX name: `--disk=`*`mpx.vmhba1:C0:T0:L0`*
- VML name: `--disk=`*`vml.000000034211234`*
- vmkLUN UID: `--disk=`*`vmkLUN_UID`*

For accepted disk name formats, see "Disk Device Names," on page 193.

--firstdisk=

***disk-type1*,**

[*disk-type2*,...] Partitions the first eligible disk found. By default, the eligible disks are set to the following order:

1 Locally attached storage (`local`)

2 Network storage (`remote`)

3 USB disks (`usb`)

You can change the order of the disks by using a comma separated list appended to the argument. If you provide a filter list, the default settings are overridden. You can combine filters to specify a particular disk, including `esx` for the first disk with ESX installed on it, model and vendor information, or the name of the vmkernel device driver. For example, to prefer a disk with the model name ST3120814A and any disk that uses the mptsas driver rather than a normal local disk, the argument is `--firstdisk=ST3120814A,mptsas,local`.

--overwritevsan You must use the `--overwritevsan` option when you install ESXi on a disk, either SSD or HDD (magnetic), that is in a Virtual SAN disk group. If you use this option and there is no Virtual SAN partition on the selected disk, the installation will fail. When you install ESXi on a disk that is in Virtual SAN disk group, the result depends on the disk you select:

- If you select an SSD, the SSD and all underlying HDDs in the same disk group will be wiped.
- If you select an HDD, and the disk group size is greater than two, only the selected HDD will be wiped.
- If you select an HDD disk, and the disk group size is two or less, the SSD and the selected HDD will be wiped.

For more information about managing Virtual SAN disk groups, see the *vSphere Storage* documentation.

--overwritevmfs

Install ESXi if a VMFS partition exists on the disk, but no ESX or ESXi installation exists. Unless this option is present, the installer will fail if a VMFS partition exists on the disk, but no ESX or ESXi installation exists.

--forcemigrate

If a version 4.x host contains customizations, such as third-party VIBS or drivers, that are not included in the installer .ISO, the installer exits with an error describing the problem. The `forcemigrate` option overrides the error and forces the upgrade.

If you are upgrading a 5.0.x host, supported custom VIBs on the host that are not included in the ESXi installer ISO are migrated. If the host or the installer .ISO contains a VIB that creates a conflict and prevents the upgrade, an error message identifies the offending VIB. You can remove the VIB and retry the upgrade, or use ESXI Image Builder to create a custom installer .ISO that resolves the conflict. The `forcemigrate` option is not available.

See "Upgrading Hosts That Have Third-Party Custom VIBs," on page 151

CAUTION Using the `forcemigrate` option might cause the upgraded host to not boot properly, to exhibit system instability, or to lose functionality.

keyboard (optional)

Sets the keyboard type for the system.

keyboardType

Specifies the keyboard map for the selected keyboard type. *keyboardType* must be one of the following types.

- Belgian
- Brazilian
- Croatian
- Czechoslovakian
- Danish
- Default
- Estonian
- Finnish
- French
- German
- Greek
- Icelandic
- Italian
- Japanese
- Latin American
- Norwegian
- Polish
- Portuguese
- Russian

- Slovenian
- Spanish
- Swedish
- Swiss French
- Swiss German
- Turkish
- US Dvorak
- Ukrainian
- United Kingdom

serialnum or vmserialnum (optional)

Deprecated in ESXi 5.0.x. Supported in ESXi 5.1. Configures licensing. If not included, ESXi installs in evaluation mode.

--esx=<license-key>	Specifies the vSphere license key to use. The format is 5 five-character groups (XXXXX-XXXXX-XXXXX-XXXXX-XXXXX).

network (optional)

Specify a network address for the system.

--bootproto=[dhcp|static]	Specify whether to obtain the network settings from DHCP or set them manually.
--device=	Specifies either the MAC address of the network card or the device name, in the form `vmnicNN`, as in `vmnic0`. This options refers to the uplink device for the virtual switch.
--ip=	Sets an IP address for the machine to be installed, in the form `xxx.xxx.xxx.xxx`. Required with the `--bootproto=static` option and ignored otherwise.
--gateway=	Designates the default gateway as an IP address, in the form `xxx.xxx.xxx.xxx`. Used with the `--bootproto=static` option.
--nameserver=	Designates the primary name server as an IP address. Used with the `--bootproto=static` option. Omit this option if you do not intend to use DNS. The `--nameserver` option can accept two IP addresses. For example: `--nameserver="10.126.87.104[,10.126.87.120]"`
--netmask=	Specifies the subnet mask for the installed system, in the form `255.xxx.xxx.xxx`. Used with the `--bootproto=static` option.
--hostname=	Specifies the host name for the installed system.
--vlanid= ***vlanid***	Specifies which VLAN the system is on. Used with either the `--bootproto=dhcp` or `--bootproto=static` option. Set to an integer from 1 to 4096.
--addvmportgroup=(0|1)	Specifies whether to add the VM Network port group, which is used by virtual machines. The default value is 1.

paranoid (optional)

Causes warning messages to interrupt the installation. If you omit this command, warning messages are logged.

part or partition (optional)

Creates an additional VMFS datastore on the system. Only one datastore per disk can be created. Cannot be used on the same disk as the `install` command. Only one partition can be specified per disk and it can only be a VMFS partition

datastore name	Specifies where the partition is to be mounted
--ondisk= or --ondrive=	Specifies the disk or drive where the partition is created.
--firstdisk= ***disk-type1*****,** **[*****disk-type2*****,...]**	Partitions the first eligible disk found. By default, the eligible disks are set to the following order: 1 Locally attached storage (`local`) 2 Network storage (`remote`) 3 USB disks (`usb`) You can change the order of the disks by using a comma separated list appended to the argument. If you provide a filter list, the default settings are overridden. You can combine filters to specify a particular disk, including `esx` for the first disk with ESX installed on it, model and vendor information, or the name of the vmkernel device driver. For example, to prefer a disk with the model name ST3120814A and any disk that uses the mptsas driver rather than a normal local disk, the argument is `--firstdisk=ST3120814A,mptsas,local`.

reboot (optional)

Reboots the machine after the scripted installation is complete.

<--noeject>	The CD is not ejected after the installation.

rootpw (required)

Sets the root password for the system.

--iscrypted	Specifies that the password is encrypted.
password	Specifies the password value.

upgrade

Either the `install`, `upgrade`, or `installorupgrade` command is required to determine which disk to install or upgrade ESXi on.

--disk= or --drive=	Specifies the disk to partition. In the command `--disk=`*`diskname`*, the *diskname* can be in any of the forms shown in the following examples: ■ Path: `--disk=`*`/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0`* ■ MPX name: `--disk=`*`mpx.vmhba1:C0:T0:L0`* ■ VML name: `--disk=`*`vml.000000034211234`*

- vmkLUN UID:`--disk=vmkLUN_UID`

For accepted disk name formats, see "Disk Device Names," on page 193.

`--firstdisk=`
`disk-type1,`
`[`*`disk-type2`*`,...]`

Partitions the first eligible disk found. By default, the eligible disks are set to the following order:

1 Locally attached storage (`local`)

2 Network storage (`remote`)

3 USB disks (`usb`)

You can change the order of the disks by using a comma separated list appended to the argument. If you provide a filter list, the default settings are overridden. You can combine filters to specify a particular disk, including `esx` for the first disk with ESX installed on it, model and vendor information, or the name of the vmkernel device driver. For example, to prefer a disk with the model name ST3120814A and any disk that uses the mptsas driver rather than a normal local disk, the argument is `--firstdisk=ST3120814A,mptsas,local`.

`--deletecosvmdk`

If the system is being upgraded from ESX, remove the directory that contains the old Service Console VMDK file, `cos.vmdk`, to reclaim unused space in the VMFS datastore.

`--forcemigrate`

If an ESX/ESXi 4.x host contains customizations, such as third-party VIBS or drivers, that are not included in the installer .ISO, the installer exits with an error describing the problem. The `forcemigrate` option overrides the error and forces the upgrade. If you are upgrading a 5.0.x host, supported custom VIBs that are not included in the ESXi installer ISO are migrated. You do not need to use the `forcemigrate` option.

See "Upgrading Hosts That Have Third-Party Custom VIBs," on page 151

CAUTION Using the `forcemigrate` option might cause the upgraded host to not boot properly, to exhibit system instability, or to lose functionality.

%include or include (optional)

Specifies another installation script to parse. This command is treated similarly to a multiline command, but takes only one argument.

`filename` For example: `%include part.cfg`

%pre (optional)

Specifies a script to run before the kickstart configuration is evaluated. For example, you can use it to generate files for the kickstart file to include.

`--interpreter`
`=[python|busybox]`

Specifies an interpreter to use. The default is busybox.

%post (optional)

Runs the specified script after package installation is complete. If you specify multiple `%post` sections, they run in the order that they appear in the installation script.

`--interpreter`

Specifies an interpreter to use. The default is busybox.

=[python|busybox]	
--timeout=secs	Specifies a timeout for running the script. If the script is not finished when the timeout expires, the script is forcefully terminated.
--ignorefailure =[true|false]	If true, the installation is considered a success even if the `%post` script terminated with an error.

%firstboot

Creates an `init` script that runs only during the first boot. The script has no effect on subsequent boots. If multiple `%firstboot` sections are specified, they run in the order that they appear in the kickstart file.

NOTE You cannot check the semantics of `%firstboot` scripts until the system is booting for the first time. A `%firstboot` script might contain potentially catastrophic errors that are not exposed until after the installation is complete.

--interpreter =[python|busybox]	Specifies an interpreter to use. The default is busybox.

NOTE You cannot check the semantics of the `%firstboot` script until the system boots for the first time. If the script contains errors, they are not exposed until after the installation is complete.

Differences Between ESXi 4.x and ESXi 5.x Scripted Installation and Upgrade Commands

Before you perform a scripted ESXi installation or upgrade, if you are familiar with ESXi version 4.x scripted installation, note the differences between ESXi 4.x and ESXi 5.x scripted installation and upgrade commands.

In ESXi 5.x, because the installation image is loaded directly into the host RAM when the host boots, you do not need to include the location of the installation media in the installation script.

ESXi 5.x supports scripted upgrades in addition to scripted installation.

Command differences are noted in the following summary.

accepteula or vmaccepteula	Only in ESXi
autopart	Deprecated and replaced with `install`, `upgrade`, or `installorupgrade`.
auth or authconfig	Not supported in ESXi 5.x.
bootloader	Not supported in ESXi 5.x.
esxlocation	Deprecated and unused in ESXi.
firewall	Not supported in ESXi 5.x.
firewallport	Not supported in ESXi 5.x.
install, installorupgrade, upgrade	These commands replace the deprecated autopart command. Use one of these command to specify the disk to partition, and the `part` command to create the vmfs datastore. `installorupgrade` and `upgrade` are newly supported in ESXi 5.x.
serialnum	Deprecated in ESXi 5.0.x. Supported in ESXi 5.1.
vmserialnum	Deprecated in ESXi 5.0.x. Supported in ESXi 5.1.
timezone	Not supported in ESXi 5.x.

virtualdisk	Not supported in ESXi 5.x.
zerombr	Not supported in ESXi 5.x.
%firstboot	--level option not supported in ESXi 5.x.
%packages	Not supported in ESXi 5.x.

Disk Device Names

The install, upgrade, and installorupgrade installation script commands require the use of disk device names.

Table 7-6. Disk Device Names

Format	Examples	Description
VML	vml.00025261	The device name as reported by the vmkernel
MPX	mpx.vmhba0:C0:T0:L0	The device name

NOTE When you perform a scripted upgrade from ESX 4.x to ESXi 5.x, the MPX and VML disk names change, which might cause the upgrade to fail. To avoid this problem, use Network Address Authority Identifiers (NAA IDs) for the disk device instead of MPX and VML disk names.

After you obtain the NAA ID or VML number, typically from the BIOS of the storage adapter, you can modify the kickstart file (ks.cfg) for each host to identify the disk device by the NAA ID or VML number.

Some devices do not provide an NAA ID. In these circumstances, an MPX Identifier is generated by ESXi to represent the LUN or disk. The identifier takes a form similar to the canonical name of previous versions of ESXi with the mpx. prefix. This identifier can be used exactly as the NAA ID. See Knowledge Base article 1014953.

About the boot.cfg File

The boot loader configuration file boot.cfg specifies the kernel, the kernel options, and the boot modules that the mboot.c32 boot loader uses in an ESXi installation.

The boot.cfg file is provided in the ESXi installer. You can modify the kernelopt line of the boot.cfg file to specify the location of an installation script or to pass other boot options.

The boot.cfg file has the following syntax:

```
# boot.cfg -- mboot configuration file
#
# Any line preceded with '#' is a comment.

title=STRING
kernel=FILEPATH
kernelopt=STRING
modules=FILEPATH1 --- FILEPATH2... --- FILEPATHn

# Any other line must remain unchanged.
```

The commands in boot.cfg configure the boot loader.

Table 7-7. Commands in boot.cfg .

Command	Description
title=*STRING*	Sets the boot loader title to *STRING*.
kernel=*FILEPATH*	Sets the kernel path to *FILEPATH*.

Table 7-7. Commands in `boot.cfg` . (Continued)

Command	Description
`kernelopt=STRING`	Appends *STRING* to the kernel boot options.
`modules=FILEPATH1 --- FILEPATH2... --- FILEPATHn`	Lists the modules to be loaded, separated by three hyphens (---).

See "Create an Installer ISO Image with a Custom Installation or Upgrade Script," on page 157, "PXE Boot the ESXi Installer by Using PXELINUX and a PXE Configuration File," on page 161, "PXE Boot the ESXi Installer by Using PXELINUX and an isolinux.cfg PXE Configuration File," on page 163, and "PXE Booting the ESXi Installer," on page 158.

Install, Upgrade, or Migrate ESXi from a CD or DVD Using a Script

You can install, upgrade, or migrate ESXi from a CD/DVD drive using a script that specifies the installation or upgrade options.

You can start the installation or upgrade script by entering a boot option when you start the host. You can also create an installer ISO image that includes the installation script. With an installer ISO image, you can perform a scripted, unattended installation when you boot the resulting installer ISO image. See "Create an Installer ISO Image with a Custom Installation or Upgrade Script," on page 157.

IMPORTANT After you upgrade or migrate your host from ESX/ESXi 4.x to ESXi 5.x, you cannot roll back to your version 4.x ESX or ESXi software. Back up your host before you perform an upgrade or migration, so that, if the upgrade or migration fails, you can restore your 4.x host.

Prerequisites

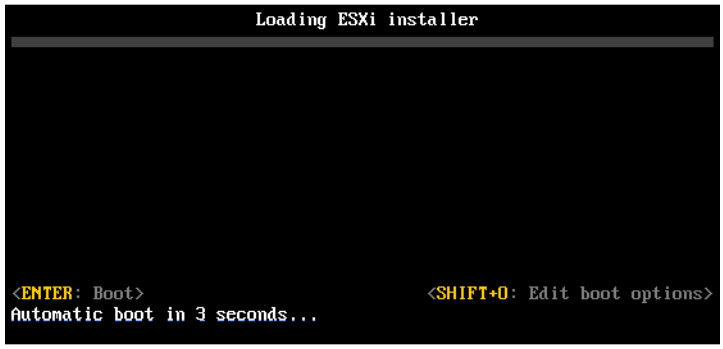
Before you run the scripted installation, upgrade, or migration, verify that the following prerequisites are met:

- The system on which you are installing, upgrading, or migrating meets the hardware requirements. See "ESXi Hardware Requirements," on page 13.
- You have the ESXi installer ISO on an installation CD/DVD. See "Download and Burn the ESXi Installer ISO Image to a CD or DVD," on page 154.
- The default installation or upgrade script (`ks.cfg`) or a custom installation or upgrade script is accessible to the system. See "About Installation and Upgrade Scripts," on page 184.
- You have selected a boot command to run the scripted installation, upgrade or migration. See "Enter Boot Options to Start an Installation or Upgrade Script," on page 182. For a complete list of boot commands, see "Boot Options," on page 183.

Procedure

1 Boot the ESXi installer from the CD or DVD using the local CD/DVD-ROM drive.

2 When the ESXi installer window appears, press Shift+O to edit boot options.



3 Type a boot option that calls the default installation or upgrade script or an installation or upgrade script file that you created.

The boot option has the form `ks=`.

4 Press Enter.

The installation, upgrade, or migration runs, using the options that you specified.

Install, Upgrade, or Migrate ESXi from a USB Flash Drive Using a Script

You can install, upgrade, or migrate ESXi from a USB flash drive using a script that specifies the installation or upgrade options.

IMPORTANT After you upgrade or migrate your host from ESX/ESXi 4.x to ESXi 5.x, you cannot roll back to your version 4.x ESX or ESXi software. Back up your host before you perform an upgrade or migration, so that, if the upgrade or migration fails, you can restore your 4.x host.

Supported boot options are listed in "Boot Options," on page 183.

Prerequisites

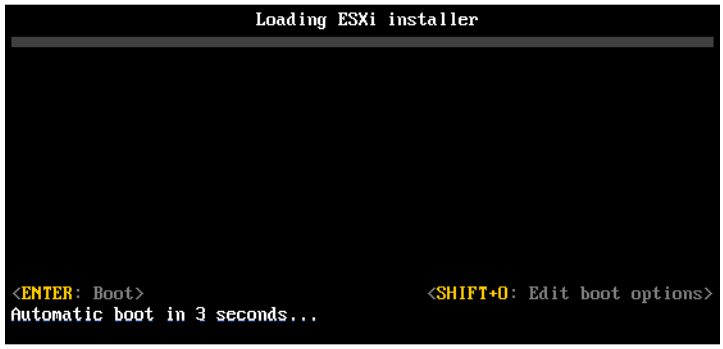
Before running the scripted installation, upgrade, or migration, verify that the following prerequisites are met:

- The system that you are installing, upgrading, or migrating to ESXi meets the hardware requirements for the installation or upgrade. See "ESXi Hardware Requirements," on page 13.
- You have the ESXi installer ISO on a bootable USB flash drive. See "Format a USB Flash Drive to Boot the ESXi Installation or Upgrade," on page 155.
- The default installation or upgrade script (`ks.cfg`) or a custom installation or upgrade script is accessible to the system. See "About Installation and Upgrade Scripts," on page 184.
- You have selected a boot option to run the scripted installation, upgrade, or migration. See "Enter Boot Options to Start an Installation or Upgrade Script," on page 182.

Procedure

1 Boot the ESXi installer from the USB flash drive.

2 When the ESXi installer window appears, press Shift+O to edit boot options.



3 Type a boot option that calls the default installation or upgrade script or an installation or upgrade script file that you created.

The boot option has the form `ks=`.

4 Press Enter.

The installation, upgrade, or migration runs, using the options that you specified.

Performing a Scripted Installation or Upgrade of ESXi by PXE Booting the Installer

ESXi 5.x provides many options for PXE booting the installer and using an installation or upgrade script.

- For information about setting up a PXE infrastructure, see "PXE Booting the ESXi Installer," on page 158.
- For information about creating and locating an installation script, see "About Installation and Upgrade Scripts," on page 184.
- For specific procedures to PXE boot the ESXi installer and use an installation script, see one of the following topics:
  - "PXE Boot the ESXi Installer by Using PXELINUX and an isolinux.cfg PXE Configuration File," on page 163
  - "PXE Boot the ESXi Installer by Using PXELINUX and a PXE Configuration File," on page 161
  - "PXE Boot the ESXi Installer Using gPXE," on page 164
- For information about using Auto Deploy to perform a scripted upgrade by PXE booting, see "Using vSphere Auto Deploy to Reprovision Hosts," on page 196.

Using vSphere Auto Deploy to Reprovision Hosts

If a host was deployed using vSphere Auto Deploy, you can use Auto Deploy to reprovision the host with a new image profile that contains an ESXi upgrade. You can use vSphere ESXi Image Builder PowerCLI to create and manage image profiles.

These instructions assume that you are reprovisioning a host that has already been provisioned with Auto Deploy. Provisioning a host that has never been provisioned with Auto Deploy differs from the process described here to upgrade a host. For information about using vSphere Auto Deploy and ESXi Image Builder PowerCLI, see the information about using vSphere Auto Deploy and vSphere ESXi Image Builder CLI in the *vSphere Installation and Setup* documentation.

Reprovisioning Hosts

vSphere Auto Deploy supports multiple reprovisioning options. You can perform a simple reboot or reprovision with a different image profile or a different host profile.

A first boot using Auto Deploy requires that you set up your environment and add rules to the rule set. See the topic "Preparing for vSphere Auto Deploy" in the *vSphere installation and Setup* documentation.

The following reprovisioning operations are available.

- Simple reboot.
- Reboot of hosts for which the user answered questions during the boot operation.
- Reprovision with a different image profile.
- Reprovision with a different host profile.

Reprovision Hosts with Simple Reboot Operations

A simple reboot of a host that is provisioned with Auto Deploy requires only that all prerequisites are still met. The process uses the previously assigned image profile, host profile, and vCenter Server location.

Setup includes DHCP server setup, writing rules, and making an image profile available to the Auto Deploy infrastructure.

Prerequisites

Make sure the setup you performed during the first boot operation is in place.

Procedure

1 Check that the image profile and host profile for the host are still available, and that the host has the identifying information (asset tag, IP address) it had during previous boot operations.

2 Place the host in maintenance mode.

Host Type	Action
Host is part of a DRS cluster	VMware DRS migrates virtual machines to appropriate hosts when you place the host in maintenance mode.
Host is not part of a DRS cluster	You must migrate all virtual machines to different hosts and place each host in maintenance mode.

3 Reboot the host.

The host shuts down. When the host reboots, it uses the image profile that the Auto Deploy server provides. The Auto Deploy server also applies the host profile stored on the vCenter Server system.

Reprovision a Host with a New Image Profile

You can reprovision the host with a new image profile, host profile, or vCenter Server location by changing the rule for the host and performing a test and repair compliance operation.

Several options for reprovisioning hosts exist.

- If the VIBs that you want to use support live update, you can use an `esxcli software vib` command. In that case, you must also update the rule set to use an image profile that includes the new VIBs.
- During testing, you can apply an image profile to an individual host with the `Apply-EsxImageProfile` cmdlet and reboot the host so the change takes effect. The `Apply-EsxImageProfile` cmdlet updates the association between the host and the image profile but does not install VIBs on the host.
- In all other cases, use this procedure.

Prerequisites

- Create the image profile you want boot the host with. Use the Image Builder PowerCLI. See "Using vSphere ESXi Image Builder CLI" in the *vSphere Installation and Setup* documentation.
- Make sure that the setup that you performed during the first boot operation is in place.

Procedure

1 At the PowerShell prompt, run the `Connect-VIServer` PowerCLI cmdlet to connect to the vCenter Server system that Auto Deploy is registered with.

```
Connect-VIServer myVCServer
```

The cmdlet might return a server certificate warning. In a production environment, make sure no server certificate warnings result. In a development environment, you can ignore the warning.

2 Determine the location of a public software depot that contains the image profile that you want to use, or define a custom image profile with the Image Builder PowerCLI.

3 Run `Add-EsxSoftwareDepot` to add the software depot that contains the image profile to the PowerCLI session.

Depot Type	Cmdlet
Remote depot	Run **`Add-EsxSoftwareDepot`** ***`depot_url`***.
ZIP file	a Download the ZIP file to a local file path or create a mount point local to the PowerCLI machine. b Run **`Add-EsxSoftwareDepot C:\`*`file_path`*`\`*`my_offline_depot`*`.zip`**.

4 Run `Get-EsxImageProfile` to see a list of image profiles, and decide which profile you want to use.

5 Run `Copy-DeployRule` and specify the `ReplaceItem` parameter to change the rule that assigns an image profile to hosts.

The following cmdlet replaces the current image profile that the rule assigns to the host with the *my_new_imageprofile* profile. After the cmdlet completes, `myrule` assigns the new image profile to hosts. The old version of `myrule` is renamed and hidden.

```
Copy-DeployRule myrule -ReplaceItem my_new_imageprofile
```

6 Test and repair rule compliance for each host that you want to deploy the image to.

See "Test and Repair Rule Compliance," on page 199.

When you reboot hosts after compliance repair, Auto Deploy provisions the hosts with the new image profile.

Assign a Host Profile to Hosts

Auto Deploy can assign a host profile to one or more hosts. The host profile might include information about storage configuration, network configuration, or other characteristics of the host. If you add a host to a cluster, that cluster's host profile is used.

The following procedure explains how to write a rule that assigns a host profile to hosts. To assign the host profiles to hosts already provisioned with Auto Deploy, you must also perform a test and repair cycle. See "Test and Repair Rule Compliance," on page 199.

In many cases, you assign a host to a cluster instead of specifying a host profile explicitly. The host uses the host profile of the cluster.

Prerequisites

- Install vSphere PowerCLI and all prerequisite software.
- Export the host profile that you want to use.
- If you encounter problems running PowerCLI cmdlets, consider changing the execution policy. See the information about using Auto Deploy Cmdlets in the *vSphere Installation and Setup* documentation.

Procedure

1 Run the `Connect-VIServer` PowerCLI cmdlet to connect to the vCenter Server system that Auto Deploy is registered with.

```
Connect-VIServer 192.XXX.X.XX
```

The cmdlet might return a server certificate warning. In a production environment, make sure no server certificate warnings result. In a development environment, you can ignore the warning.

2 Using the vSphere Web Client, set up a host with the settings you want to use and create a host profile from that host.

3 Find the name of the host profile by running `Get-VMhostProfile` PowerCLI cmdlet, passing in the ESXi host from which you create a host profile.

4 At the PowerCLI prompt, define a rule in which hosts with certain attributes, for example a range of IP addresses, are assigned to the host profile.

```
New-DeployRule -Name "testrule2" -Item my_host_profile -Pattern "vendor=Acme,Zven",
"ipv4=192.XXX.1.10-192.XXX.1.20"
```

The specified item is assigned to all hosts with the specified attributes. This example specifies a rule named testrule2. The rule assigns the specified host profile my_host_profile to all hosts with an IP address inside the specified range and with a manufacturer of Acme or Zven.

5 Add the rule to the rule set.

```
Add-DeployRule testrule2
```

By default, the working rule set becomes the active rule set, and any changes to the rule set become active when you add a rule. If you use the `NoActivate` parameter, the working rule set does not become the active rule set.

What to do next

- Upgrade existing hosts to use the new host profile by performing compliance test and repair operations on those hosts. See "Test and Repair Rule Compliance," on page 199.
- Turn on unprovisioned hosts to provision them with the host profile.

Test and Repair Rule Compliance

When you add a rule to the Auto Deploy rule set or make changes to one or more rules, hosts are not updated automatically. Auto Deploy applies the new rules only when you test their rule compliance and perform remediation.

This task assumes that your infrastructure includes one or more ESXi hosts provisioned with Auto Deploy, and that the host on which you installed vSphere PowerCLI can access those ESXi hosts.

Prerequisites

- Install vSphere PowerCLI and all prerequisite software.
- If you encounter problems running PowerCLI cmdlets, consider changing the execution policy. See the information about using Auto Deploy Cmdlets in the *vSphere Installation and Setup* documentation.

Procedure

1 Use PowerCLI to check which Auto Deploy rules are currently available.

```
Get-DeployRule
```

The system returns the rules and the associated items and patterns.

2 Make a change to one of the available rules, for example, you might change the image profile and the name of the rule.

```
Copy-DeployRule -DeployRule testrule -ReplaceItem MyNewProfile
```

You cannot edit a rule already added to a rule set. Instead, you copy the rule and replace the item or pattern you want to change. By default, PowerCLI uses the old name for the copy and hides the old rule.

3 Verify that the host that you want to test rule set compliance for is accessible.

```
Get-VMHost -Name MyEsxi42
```

4 Run the cmdlet that tests rule set compliance for the host, and bind the return value to a variable for later use.

```
$tr = Test-DeployRuleSetCompliance MyEsxi42
```

5 Examine the differences between what is in the rule set and what the host is currently using.

```
$tr.itemlist
```

The system returns a table of current and expected items.

```
CurrentItem                          ExpectedItem
-----------                          ------------
My Profile 25                        MyProfileUpdate
```

6 Remediate the host to use the revised rule set the next time you boot the host.

```
Repair-DeployRuleSetCompliance $tr
```

What to do next

If the rule you changed specified the inventory location, the change takes effect when you repair compliance. For all other changes, boot your host to have Auto Deploy apply the new rule and to achieve compliance between the rule set and the host.

Upgrading Hosts by Using esxcli Commands

Using the vSphere CLI, you can upgrade, update, or patch ESXi 5.x hosts.

You cannot use `esxcli` commands to upgrade version 4.x ESX or ESXi hosts to ESXi 5.x. To upgrade version 4.x ESX or ESXi hosts to ESXi 5.x, use vSphere Update Manager, or perform an interactive or scripted upgrade.

To use esxcli vCLI commands, you must install vSphere CLI (vCLI). For more information about installing and using the vSphere CLI, see the following documents:

- *Getting Started with vSphere Command-Line Interfaces*
- *vSphere Command-Line Interface Concepts and Examples*

- *vSphere Command-Line Interface Reference* is a reference to `vicfg-` and related vCLI commands.

NOTE If you press Ctrl+C while an `esxcli` command is running, the command-line interface exits to a new prompt without displaying a message. However, the command continues to run to completion.

For ESXi hosts deployed with vSphere Auto Deploy, the tools VIB must be part of the base booting image used for the initial Auto Deploy installation. The tools VIB cannot be added separately later.

VIBs, Image Profiles, and Software Depots

Upgrading ESXi with esxcli commands requires an understanding of VIBs, image profiles, and software depots.

The following technical terms are used throughout the vSphere documentation set in discussions of installation and upgrade tasks.

VIB — A VIB is an ESXi software package. VMware and its partners package solutions, drivers, CIM providers, and applications that extend the ESXi platform as VIBs. VIBs are available in software depots. You can use VIBs to create and customize ISO images or to upgrade ESXi hosts by installing VIBs asynchronously onto the hosts.

Image Profile — An image profile defines an ESXi image and consists of VIBs. An image profile always includes a base VIB, and might include more VIBs. You examine and define an image profile using the Image Builder PowerCLI.

Software Depot — A software depot is a collection of VIBs and image profiles. The software depot is a hierarchy of files and folders and can be available through an HTTP URL (online depot) or a ZIP file (offline depot). VMware and VMware partners make depots available. Companies with large VMware installations might create internal depots to provision ESXi hosts with vSphere Auto Deploy, or to export an ISO for ESXi installation.

Understanding Acceptance Levels for VIBS and Hosts

Each VIB is released with an acceptance level that cannot be changed. The host acceptance level determines which VIBs can be installed to a host.

The acceptance level applies to individual VIBs installed by using the `esxcli software vib install` and `esxcli software vib update` commands, to VIBs installed using vSphere Update Manager, and to VIBs in image profiles.

The acceptance level of all VIBs on a host must be at least as high as the host acceptance level. For example, if the host acceptance level is VMwareAccepted, you can install VIBs with acceptance levels of VMwareCertified and VMwareAccepted, but you cannot install VIBs with acceptance levels of PartnerSupported or CommunitySupported. To install a VIB with a less restrictive acceptance level than that of the host, you can change the acceptance level of the host by using the vSphere Web Client or by running `esxcli software acceptance` commands.

Setting host acceptance levels is a best practice that allows you to specify which VIBs can be installed on a host and used with an image profile, and the level of support you can expect for a VIB. For example, you would probably set a more restrictive acceptance level for hosts in a production environment than for hosts in a testing environment.

VMware supports the following acceptance levels.

VMwareCertified The VMwareCertified acceptance level has the most stringent requirements. VIBs with this level go through thorough testing fully equivalent to VMware in-house Quality Assurance testing for the same technology. Today, only IOVP drivers are published at this level. VMware takes support calls for VIBs with this acceptance level.

VMwareAccepted VIBs with this acceptance level go through verification testing, but the tests do not fully test every function of the software. The partner runs the tests and VMware verifies the result. Today, CIM providers and PSA plugins are among the VIBs published at this level. VMware directs support calls for VIBs with this acceptance level to the partner's support organization.

PartnerSupported VIBs with the PartnerSupported acceptance level are published by a partner that VMware trusts. The partner performs all testing. VMware does not verify the results. This level is used for a new or nonmainstream technology that partners want to enable for VMware systems. Today, driver VIB technologies such as Infiniband, ATAoE, and SSD are at this level with nonstandard hardware drivers. VMware directs support calls for VIBs with this acceptance level to the partner's support organization.

CommunitySupported The Community Supported acceptance level is for VIBs created by individuals or companies outside of VMware partner programs. VIBs at this level have not gone through any VMware-approved testing program and are not supported by VMware Technical Support or by a VMware partner.

Table 7-8. VIB Acceptance Levels Required to Install on Hosts

Host Acceptance Level	VMwareCertified VIB	VMwareAccepted VIB	PartnerSupported VIB	CommunitySupported VIB
VMwareCertified	x			
VMwareAccepted	x	x		
PartnerSupported	x	x	x	
CommunitySupported	x	x	x	x

Match a Host Acceptance Level with an Update Acceptance Level

You can change the host acceptance level to match the acceptance level for a VIB or image profile that you want to install. The acceptance level of all VIBs on a host must be at least as high as the host acceptance level.

Use this procedure to determine the acceptance levels of the host and the VIB or image profile to install, and to change the acceptance level of the host, if necessary for the update.

When you specify a target server by using **`--server=server_name`** in the procedure, the specified server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with vSphere Command-Line Interfaces*, or run `esxcli --help` at the vCLI command prompt.

Prerequisites

Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See *Getting Started with vSphere Command-Line Interfaces*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

Procedure

1 Retrieve the acceptance level for the VIB or image profile.

Option	Description
List information for all VIBs	`esxcli --server=server_name software sources vib list --depot=depot_URL`
List information for a specified VIB	`esxcli --server=server_name software sources vib list --viburl=vib_URL`
List information for all image profiles	`esxcli --server=server_name software sources profile list --depot=depot_URL`
List information for a specified image profile	`esxcli --server=server_name software sources profile get --depot=depot_URL --profile=profile_name`

2 Retrieve the host acceptance level.

```
esxcli --server=server_name software acceptance get
```

3 (Optional) If the acceptance level of the VIB is more restrictive than the acceptance level of the host, change the acceptance level of the host.

```
esxcli --server=server_name software acceptance set --level=acceptance_level
```

The *acceptance_level* can be `VMwareCertified`, `VMwareAccepted`, `PartnerSupported`, or `CommunitySupported`. The values for *acceptance_level* are case-sensitive.

NOTE You can use the `--force` option for the `esxcli software vib` or `esxcli software profile` command to add a VIB or image profile with a lower acceptance level than the host. A warning will appear. Because your setup is no longer consistent, the warning is repeated when you install VIBs, remove VIBs, and perform certain other operations on the host.

Determine Whether an Update Requires the Host to Be in Maintenance Mode or to Be Rebooted

VIBs that you can install with live install do not require the host to be rebooted, but might require the host to be placed in maintenance mode. Other VIBs and profiles might require the host to be rebooted after the installation or update.

When you specify a target server by using **`--server=server_name`** in the procedure, the specified server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with vSphere Command-Line Interfaces*, or run `esxcli --help` at the vCLI command prompt.

Prerequisites

Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See *Getting Started with vSphere Command-Line Interfaces*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

Procedure

1 Check whether the VIB or image profile that you want to install requires the host to be placed in maintenance mode or to be rebooted after the installation or update.

Run one of the following commands.

Option	Description
Check the VIB	`esxcli --server=server_name software sources vib get -v absolute_path_to_vib`
Check the VIBs in a depot	`esxcli --server=server_name software sources vib get --depot=depot_name`
Check the image profile in a depot	`esxcli --server=server_name software sources profile get --depot=depot_name`

2 Review the return values.

The return values, which are read from the VIB metadata, indicate whether the host must be in maintenance mode before installing the VIB or image profile, and whether installing the VIB or profile requires the host to be rebooted.

NOTE vSphere Update Manager relies on the `esxupdate`/`esxcli` scan result to determine whether maintenance mode is required or not. When you install a VIB on a live system, if the value for `Live-Install-Allowed` is set to false, the installation result will instruct Update Manager to reboot the host. When you remove a VIB from a live system, if the value for `Live-Remove-Allowed` is set to false, the removal result will instruct Update Manager to reboot the host. In either case, during the reboot, Update Manager will automatically put the host into maintenance mode.

What to do next

If necessary, place the host in maintenance mode. See "Place a Host in Maintenance Mode," on page 204. If a reboot is required, and if the host belongs to a VMware HA cluster, remove the host from the cluster or disable HA on the cluster before the installation or update.

Place a Host in Maintenance Mode

Some installation and update operations that use live install require the host to be in maintenance mode.

To determine whether an upgrade operation requires the host to be in maintenance mode, see "Determine Whether an Update Requires the Host to Be in Maintenance Mode or to Be Rebooted," on page 203

NOTE If the host is a member of a Virtual SAN cluster, and any virtual machine object on the host uses the "Number of failures to tolerate=0" setting in its storage policy, the host might experience unusual delays when entering maintenance mode. The delay occurs because Virtual SAN has to evacuate this object from the host for the maintenance operation to complete successfully.

When you specify a target server by using **`--server=server_name`** in the procedure, the specified server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with vSphere Command-Line Interfaces*, or run `esxcli --help` at the vCLI command prompt.

Prerequisites

Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See *Getting Started with vSphere Command-Line Interfaces*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

Procedure

1 Check to determine whether the host is in maintenance mode.

```
vicfg-hostops --server=server_name --operation info
```

2 Run one of the following commands for each virtual machine to power off all virtual machines running on the ESXi host.

Option	Command
To have the system try to shut down the guest operating system	`vmware-cmd --server=server_name path_to_vm stop soft`
To force the power off operation	`vmware-cmd --server=server_name path_to_vm stop hard`

Alternatively, to avoid powering off virtual machines, you can migrate them to another host. See the topic *Migrating Virtual Machines* in the *vCenter Server and Host Management* documentation.

3 Place the host in maintenance mode.

```
vicfg-hostops --server=server_name --operation enter
```

4 Verify that the host is in maintenance mode.

```
vicfg-hostops --server=server_name --operation info
```

Update a Host with Individual VIBs

You can update a host with VIBs stored in a software depot that is accessible through a URL or in an offline ZIP depot.

IMPORTANT If you are updating ESXi from a zip bundle in a VMware-supplied depot, either online from the VMware Web site or downloaded locally, VMware supports only the update method specified for VMware-supplied depots in the topic "Upgrade or Update a Host with Image Profiles," on page 206.

The **`esxcli software vib update`** and **`esxcli software vib install`** commands are not supported for upgrade operations. See "Differences Between vSphere Upgrades and Updates," on page 12 and "Upgrade or Update a Host with Image Profiles," on page 206.

When you specify a target server by using **`--server=server_name`** in the procedure, the specified server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with vSphere Command-Line Interfaces*, or run `esxcli --help` at the vCLI command prompt.

Prerequisites

- Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See *Getting Started with vSphere Command-Line Interfaces*. For troubleshooting, run `esxcli` commands in the ESXi Shell.
- Determine whether the update requires the host to be in maintenance mode or to be rebooted. If necessary, place the host in maintenance mode.

  See "Determine Whether an Update Requires the Host to Be in Maintenance Mode or to Be Rebooted," on page 203. See "Place a Host in Maintenance Mode," on page 204.
- If the update requires a reboot, and if the host belongs to a VMware HA cluster, remove the host from the cluster or disable HA on the cluster.

Procedure

1 Determine which VIBs are installed on the host.

```
esxcli --server=server_name software vib list
```

2 Find out which VIBs are available in the depot.

Option	Description
from a depot accessible by URL	`esxcli --server=server_name software sources vib list --depot=http://web_server/depot_name`
from a local depot ZIP file	`esxcli --server=server_name software sources vib list --depot=absolute_path_to_depot_zip_file`

You can specify a proxy server by using the `--proxy` argument.

3 Update the existing VIBs to include the VIBs in the depot or install new VIBs.

Option	Description
Update VIBs from a depot accessible by URL	`esxcli --server=server_name software vib update --depot=http://web_server/depot_name`
Update VIBs from a local depot ZIP file	`esxcli --server=server_name software vib update --depot=absolute_path_to_depot_ZIP_file`
Install all VIBs from a ZIP file on a specified offline depot (includes both VMware VIBs and partner-supplied VIBs)	`esxcli --server=server_name software vib install --depot path_to_VMware_vib_ZIP_file\VMware_vib_ZIP_file --depot path_to_partner_vib_ZIP_file\partner_vib_ZIP_file`

Options for the `update` and `install` commands allow you to perform a dry run, to specify a specific VIB, to bypass acceptance level verification, and so on. Do not bypass verification on production systems. See the *esxcli Reference* at http://www.vmware.com/support/developer/vcli/.

4 Verify that the VIBs are installed on your ESXi host.

```
esxcli --server=server_name software vib list
```

Upgrade or Update a Host with Image Profiles

You can upgrade or update a host with image profiles stored in a software depot that is accessible through a URL or in an offline ZIP depot.

You can use the **`esxcli software profile update`** or **`esxcli software profile install`** command to upgrade or update an ESXi host. To understand the differences between upgrades and updates, see "Differences Between vSphere Upgrades and Updates," on page 12.

When you upgrade or update a host, the **`esxcli software profile update`** or **`esxcli software profile install`** command applies a higher version (major or minor) of a full image profile onto the host. After this operation and a reboot, the host can join to a vCenter Server environment of the sdame hisgher version.

The **`esxcli software profile update`** command brings the entire contents of the ESXi host image to the same level as the corresponding upgrade method using an ISO installer. However, the ISO installer performs a pre-upgrade check for potential problems, and the **`esxcli`** upgrade method does not. The ISO installer checks the host to make sure that it has sufficient memory for the upgrade, and does not have unsupported devices connected. For more about the ISO installer and other ESXi upgrade methods, see "ESXi 5.5 Upgrade Options," on page 150.

IMPORTANT If you are upgrading or updating ESXi from a zip bundle in a VMware-supplied depot, either online from the VMware Web site or downloaded locally, VMware supports only the update command `esxcli software profile update --depot=depot_location --profile=profile_name`.

When you specify a target server by using **--server=server_name** in the procedure, the specified server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with vSphere Command-Line Interfaces*, or run `esxcli --help` at the vCLI command prompt.

NOTE Options to the `update` and `install` commands allow you to perform a dry run, to specify a specific VIB, to bypass acceptance level verification, and so on. Do not bypass verification on production systems. See the *vSphere Command-Line Interface Reference*.

Prerequisites

- Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See *Getting Started with vSphere Command-Line Interfaces*. For troubleshooting, run `esxcli` commands in the ESXi Shell.
- Determine whether the update requires the host to be in maintenance mode or to be rebooted. If necessary, place the host in maintenance mode.

  See "Determine Whether an Update Requires the Host to Be in Maintenance Mode or to Be Rebooted," on page 203. See "Place a Host in Maintenance Mode," on page 204.
- If the update requires a reboot, and if the host belongs to a VMware HA cluster, remove the host from the cluster or disable HA on the cluster.

Procedure

1 Determine which VIBs are installed on the host.

```
esxcli --server=server_name software vib list
```

2 Determine which image profiles are available in the depot.

```
esxcli --server=server_name software sources profile list --depot=http://webserver/depot_name
```

You can specify a proxy server by using the **--proxy** argument.

3 Update the existing image profile to include the VIBs or install new VIBs.

IMPORTANT The `software profile update` command updates existing VIBS with the corresponding VIBs from the specified profile, but does not affect other VIBs installed on the target server. The `software profile install` command installs the VIBs present in the depot image profile, and removes any other VIBS installed on the target server.

Option	Description
Update the image profile from a VMware-supplied zip bundle, in a depot, accessible online from the VMware Web site or downloaded to a local depot.	**esxcli software profile update --depot=*depot_location* --profile=*profile_name*** IMPORTANT This is the only update method that VMware supports for zip bundles supplied by VMware. VMware-supplied zip bundle names take the form: **VMware-ESXi-5.5.x-*build_number*-depot.zip** The profile name for VMware-supplied ziip bundles takes one of the following forms. ■ **ESXi-5.5.x-*build_number*-standard** ■ **ESXi-5.5.x-*build_number*-notools** (does not include VMware Tools)
Update the image profile from a depot accessible by URL	**esxcli --server=*server_name* software profile update --depot=http://*webserver/depot_name* --profile=*profile_name***
Update the image profile from ZIP file stored locally on the target server	**esxcli --server=*server_name* software profile update --depot=file:///<path_to_profile_ZIP_file>/<profile_ZIP_file> --profile=*profile_name***

Option	Description
Update the image profile from a ZIP file on the target server, copied into a datastore	`esxcli --server=server_name software profile update --depot="[datastore_name]profile_ZIP_file" --profile=profile_name`
Update the image profile from a ZIP file copied locally and applied on the target server	`esxcli --server=server_name software profile update --depot=/root_dir/path_to_profile_ZIP_file/profile_ZIP_file --profile=profile_name`
Install all new VIBs in a specified profile accessible by URL	`esxcli --server=server_name software profile install --depot=http://webserver/depot_name --profile=profile_name`
Install all new VIBs in a specified profile from a ZIP file stored locally on the target	`esxcli --server=server_name software profile install --depot=file:///<path_to_profile_ZIP_file>/<profile_ZIP_file> --profile=profile_name`
Install all new VIBs from a ZIP file on the target server, copied into a datastore	`esxcli --server=server_name software profile install --depot="[datastore_name]profile_ZIP_file" --profile=profile_name`
Install all new VIBs from a ZIP file copied locally and applied on the target server	`esxcli --server=server_name software profile install --depot=/root_dir/path_to_profile_ZIP_file/profile_ZIP_file --profile=profile_name`

NOTE Options to the `update` and `install` commands allow you to perform a dry run, to specify a specific VIB, to bypass acceptance level verification, and so on. Do not bypass verification on production systems. See the *vSphere Command-Line Interface Reference*.

4 Verify that the VIBs are installed on your ESXi host.

```
esxcli --server=server_name software vib list
```

Update ESXi Hosts by Using Zip Files

You can update hosts with VIBs or image profiles by downloading a ZIP file of a depot.

VMware partners prepare third-party VIBs to provide management agents or asynchronously released drivers.

IMPORTANT If you are updating ESXi from a zip bundle in a VMware-supplied depot, either online from the VMware Web site or downloaded locally, VMware supports only the update method specified for VMware-supplied depots in the topic "Upgrade or Update a Host with Image Profiles," on page 206.

The **`esxcli software vib update`** and **`esxcli software vib install`** commands are not supported for upgrade operations. See "Differences Between vSphere Upgrades and Updates," on page 12 and "Upgrade or Update a Host with Image Profiles," on page 206.

When you specify a target server by using **`--server=server_name`** in the procedure, the specified server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with vSphere Command-Line Interfaces*, or run `esxcli --help` at the vCLI command prompt.

Prerequisites

- Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See *Getting Started with vSphere Command-Line Interfaces*. For troubleshooting, run `esxcli` commands in the ESXi Shell.
- Download the ZIP file of a depot bundle from a third-party VMware partner.
- Determine whether the update requires the host to be in maintenance mode or to be rebooted. If necessary, place the host in maintenance mode.

  See "Determine Whether an Update Requires the Host to Be in Maintenance Mode or to Be Rebooted," on page 203. See "Place a Host in Maintenance Mode," on page 204.

- If the update requires a reboot, and if the host belongs to a VMware HA cluster, remove the host from the cluster or disable HA on the cluster.

Procedure

- Install the ZIP file.

  ```
  esxcli --server=server_name software vib update --depot=/path_to_vib_ZIP/ZIP_file_name.zip
  ```

Remove VIBs from a Host

You can uninstall third-party VIBs or VMware VIBs from your ESXi host.

VMware partners prepare third-party VIBs to provide management agents or asynchronously released drivers.

Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See *Getting Started with vSphere Command-Line Interfaces*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

Prerequisites

- If the removal requires a reboot, and if the host belongs to a VMware HA cluster, disable HA for the host.
- Determine whether the update requires the host to be in maintenance mode or to be rebooted. If necessary, place the host in maintenance mode.

  See "Determine Whether an Update Requires the Host to Be in Maintenance Mode or to Be Rebooted," on page 203. See "Place a Host in Maintenance Mode," on page 204.
- Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See *Getting Started with vSphere Command-Line Interfaces*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

Procedure

1. Run one of the following commands for each virtual machine to power off all virtual machines running on the ESXi host.

Option	Command
To have the system try to shut down the guest operating system	`vmware-cmd --server=server_name path_to_vm stop soft`
To force the power off operation	`vmware-cmd --server=server_name path_to_vm stop hard`

   Alternatively, to avoid powering off virtual machines, you can migrate them to another host. See the topic *Migrating Virtual Machines* in the *vCenter Server and Host Management* documentation.

2. Place the host in maintenance mode.

   ```
   vicfg-hostops --server=server_name --operation enter
   ```

3. If necessary, shut down or migrate virtual machines.
4. Determine which VIBs are installed on the host.

   ```
   esxcli --server=server_name software vib list
   ```

5. Remove the VIB.

   ```
   esxcli --server=server_name software vib remove --vibname=name
   ```

   Specify one or more VIBs to remove in one of the following forms:

   - *name*
   - *name*:*version*

- ***vendor*:*name***
- ***vendor*:*name*:*version***

For example, the command to remove a VIB specified by vendor, name and version would take this form:

```
esxcli --server myEsxiHost software vib remove --vibname=PatchVendor:patch42:version3
```

NOTE The `remove` command supports several more options. See the *vSphere Command-Line Interface Reference*.

Adding Third-Party Extensions to Hosts with esxcli

If a third-party extension is released as a VIB package, and you use the `esxcli software vib` command to add the VIB package to your system, the VIB system updates the firewall ruleset and refreshes the host daemon after you reboot your system.

Otherwise, you can use a firewall configuration file to specify port rules for host services that you want to enable for the extension. The *vSphere Security* documentation discusses how to add, apply, and refresh a firewall rule set and lists the `esxcli network firewall` commands.

The ESXi 5.x `ruleset.xml` format for ESXi 5.x is the same as in version 4.x for ESX and ESXi, but has two more tags, `enabled` and `required`. The ESXi 5.x firewall still supports the older format.

Perform a Dry Run of an esxcli Installation or Upgrade

You can use the `--dry-run` option to preview the results of an installation or upgrade operation. A dry run of the installation or update procedure does not make any changes, but reports the VIB-level operations that will be performed if you run the command without the `--dry-run` option.

When you specify a target server by using **`--server=server_name`** in the procedure, the specified server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with vSphere Command-Line Interfaces*, or run `esxcli --help` at the vCLI command prompt.

Prerequisites

Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See *Getting Started with vSphere Command-Line Interfaces*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

Procedure

1 Enter the installation or upgrade command, adding the **--dry-run** option.

- **`esxcli --server=`*`server_name`*` software vib install --dry-run`**
- **`esxcli --server=`*`server_name`*` software vib update --dry-run`**
- **`esxcli --server=`*`server_name`*` software profile install --dry-run`**
- **`esxcli --server=`*`server_name`*` software profile update --dry-run`**

2 Review the output that is returned.

The output shows which VIBs will be installed or removed and whether the installation or update requires a reboot.

Display the Installed VIBs and Profiles That Will Be Active After the Next Host Reboot

You can use the `--rebooting-image` option to list the VIBs and profiles that are installed on the host and will be active after the next host reboot.

When you specify a target server by using **`--server=server_name`** in the procedure, the specified server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with vSphere Command-Line Interfaces*, or run `esxcli --help` at the vCLI command prompt.

Prerequisites

Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See *Getting Started with vSphere Command-Line Interfaces*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

Procedure

1 Enter one of the following commands.

Option	Description
For VIBs	**`esxcli --server=server_name software vib list --rebooting-image`**
For Profiles	**`esxcli --server=server_name software profile get --rebooting-image`**

2 Review the output that is returned.

The output displays information for the ESXi image that will become active after the next reboot. If the pending-reboot image has not been created, the output returns nothing.

Display the Image Profile and Acceptance Level of the Host

You can use the `software profile get` command to display the currently installed image profile and acceptance level for the specified host.

This command also shows details of the installed image profile history, including profile modifications.

When you specify a target server by using **`--server=server_name`** in the procedure, the specified server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with vSphere Command-Line Interfaces*, or run `esxcli --help` at the vCLI command prompt.

Prerequisites

Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See *Getting Started with vSphere Command-Line Interfaces*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

Procedure

1 Enter the following command.

`esxcli --server=server_name software profile get`

2 Review the output.

Errors and Warnings Returned by the Installation and Upgrade Precheck Script

The installation and upgrade precheck script runs tests to identify problems on the host machine that can cause an installation, upgrade, or migration to fail.

For interactive installations, upgrades, and migrations, the errors or warnings are displayed on the final panel of the installer, where you are asked to confirm or cancel the installation or upgrade. For scripted installations, upgrades, or migrations, the errors or warnings are written to the installation log.

vSphere Update Manager provides custom messages for these errors or warnings. To see the original errors and warnings returned by the precheck script during an Update Manager host upgrade scan, review the Update Manager log file `vmware-vum-server-log4cpp.log`.

Table 7-9. Error and Warning Codes That Are Returned by the Installation and Upgrade Precheck Script

Error or Warning	Description
64BIT_LONGMODESTATUS	The host processor must be 64-bit.
COS_NETWORKING	Warning. An IPv4 address was found on an enabled Service Console virtual NIC for which there is no corresponding address in the same subnet in the vmkernel. A separate warning will be output for each such occurrence.
CPU_CORES	The host must have at least two cores.
DISTRIBUTED_VIRTUAL_SWITCH	If Cisco's Virtual Ethernet Module (VEM) software is found on the host, the test checks to make sure the upgrade also contains the VEM software, and that it supports the same version of the Virtual Supervisor Module (VSM) as the existing version on the host. If the software is missing or is compatible with a different version of the VSM, the test returns a warning, and the result indicates which version of the VEM software was expected on the upgrade ISO and which version, if any, were found. You can use ESXi Image Builder CLI to create a custom installation ISO that includes the appropriate version of the VEM software.
HARDWARE_VIRTUALIZATION	Warning. If the host processor doesn't have hardware virtualization or if hardware virtualization is not turned on in the host BIOS, host performance will suffer. Enable hardware virtualization in the host machine boot options. See your hardware vendor's documentation.
MD5_ROOT_PASSWORD	This test checks that the root password is encoded in MD5 format. If a password is not encoded in MD5 format, it might be significant only to eight characters. In this case, any characters after the first eight are no longer authenticated after the upgrade, which can create a security issue. To work around this problem, see VMware Knowledge Base article 1024500.
MEMORY_SIZE	The host requires the specified amount of memory to upgrade.
PACKAGE_COMPLIANCE	vSphere Update Manager only. This test checks the existing software on the host against the software contained on the upgrade ISO to determine whether the host has been successfully upgraded. If any of the packages are missing or are an older version than the package on the upgrade ISO, the test returns an error and indicates which software was found on the host, and which software was found on the upgrade ISO.

Table 7-9. Error and Warning Codes That Are Returned by the Installation and Upgrade Precheck Script (Continued)

Error or Warning	Description
PARTITION_LAYOUT	Upgrading or migration is possible only if there is at most one VMFS partition on the disk that is being upgraded and the VMFS partition must start after sector 1843200
POWERPATH	This test checks for installation of EMC PowerPath software, consisting of a CIM module and a kernel module. If either of these components is found on the host, the test checks to make sure that matching components (CIM, vmkernel module) also exist in the upgrade. If they do not, the test returns a warning that indicates which PowerPath components were expected on the upgrade ISO and which, if any, were found.
PRECHECK_INITIALIZE	This test checks that the precheck script itself can be run.
SANE_ESX_CONF	The file `/etc/vmware/esx.conf` must exist on the host.
SPACE_AVAIL_ISO	vSphere Update Manager only. The host disk must have enough free space to store the contents of the installer CD or DVD.
SPACE_AVAIL_CONFIG	vSphere Update Manager only. The host disk must have enough free space to store the 4.x configuration between reboots.
SUPPORTED_ESX_VERSION	Upgrading or migration to ESXi 5.x is possible only from version 4.x ESX hosts or version 4.x or 5.x ESXi hosts.
TBOOT_REQUIRED	This message applies only to vSphere Update Manager upgrades. The upgrade fails with this error when the host system is running in Trusted Boot mode (tboot), but the ESXi upgrade ISO does not contain any tboot VIBs. This test prevents an upgrade that can make the host less secure.
UNSUPPORTED_DEVICES	Warning. This test checks for unsupported devices. Some PCI devices are not supported in ESXi 5.x.
UPDATE_PENDING	This test checks the host for VIB installations that require a reboot. This test fails if one or more such VIBs is installed, but the host has not yet been rebooted. In these conditions, the precheck script is unable to reliably determine which packages are currently installed on the host, so it might not be safe to rely on the rest of the precheck tests to determine whether an upgrade is safe. If you encounter this error, restart the host and retry the upgrade.

After You Upgrade or Migrate Hosts

A host upgrade or migration is not complete until you have ensured that the host is reconnected to its managing vCenter Server and reconfigured if necessary, and that the host license is reapplied or upgraded.

After you upgrade or migrate a host, take the following actions:

- View the upgrade logs. You can use the vSphere Web Client to export the log files.
- If vCenter Server manages the host, you must reconnect the host to vCenter Server by right-clicking the host in the vCenter Server inventory and selecting **Connect**.
- When the upgrade is complete, ESXi is in evaluation mode. The evaluation mode period is 60 days. You must reapply your license or assign an upgraded license to your product within 60 days after the upgrade. Use the License Portal and the vSphere Web Client to configure licensing. See

- On the VMware Web site, log in to your account page to access the license portal. From the license portal, upgrade your ESXi license. Use the vSphere Web Client to assign the upgraded license key to the host.
- The host sdX devices might be renumbered after the upgrade. If necessary, update any scripts that reference sdX devices.
- After the upgrade, convert any ESX 3.x-style /adv/Disk/MaskLUNs LUN masks to the claim rule format. Run the `esxcli storage core claimrule convert` command in the vSphere Command-Line Interface (vCLI). This command converts the `/adv/Disk/MaskLUNs` advanced configuration entry in `/etc/vmware/esx.conf` to claim rules with MASK_PATH as the plug-in.

CAUTION This conversion will not work for all input MaskLUNs variations. See the *vSphere Command-Line Interface Reference*.

- Upgrade virtual machines on the host. See Chapter 8, "Upgrading Virtual Machines and VMware Tools," on page 215.

About ESXi Evaluation and Licensed Modes

You can use evaluation mode to explore the entire set of features that are available for ESXi hosts. The evaluation mode provides the set of features equal to a vSphere Enterprise Plus license. Before the evaluation mode expires, you must assign to your hosts a license that supports all the features currently in use.

For example, in evaluation mode, you can use vMotion, vSphere HA, vSphere DRS, and other features. If you want to continue using these features, you must assign a license that supports them.

The installable version of ESXi hosts is always installed in evaluation mode. ESXi Embedded is preinstalled on an internal storage device by your hardware vendor. It might be in evaluation mode or prelicensed.

The evaluation period is 60 days and begins when you turn on the ESXi host. Any time during the 60-day evaluation period, you can convert from licensed mode to evaluation mode. The time available in the evaluation period is decreased by the time already used.

For example, suppose that you use an ESXi host in evaluation mode for 20 days and then assign a vSphere Standard license key to the host. If you set the host back in evaluation mode, you can explore the entire set of features that are available for the host for the remaining evaluation period of 40 days.

For information about managing licensing for ESXi hosts, see *vCenter Server and Host Management*.

Reapplying Licenses After Upgrading to ESXi 5.5

After you upgrade to ESXi 5.5, you might need to reapply your host license.

If you upgrade from ESX/ESXi 4.x, your ESXi 5.5 software returns to the 60-day evaluation mode period until you reapply your license. See "About ESXi Evaluation and Licensed Modes," on page 214. If you upgrade from ESXi 5.0 x or 5.1.x, your existing license applies.

You can apply your license using the vSphere Web Client and vCenter Server. See the *vCenter Server and Host Management* documentation. If you use the scripted method to upgrade to ESXi 5.5, you can provide the license key in the kickstart (ks) file.

Upgrading Virtual Machines and VMware Tools

8

After you upgrade ESXi hosts, you can upgrade the virtual machines on the host to take advantage of new features.

VMware offers the following tools for upgrading virtual machines:

vSphere Web Client	Requires you to perform the virtual machine upgrade one step at a time, but does not require vSphere Update Manager. See the information about upgrading virtual machines in the *vSphere Virtual Machine Administration* documentation.
vSphere Update Manager	Automates the process of upgrading and patching virtual machines, thereby ensuring that the steps occur in the correct order. You can use Update Manager to directly upgrade the virtual machine hardware version and VMware Tools. See the *Installing and Administering VMware vSphere Update Manager* documentation.

9 Example Upgrade Scenarios

Upgrade scenarios for vSphere 4.1 include cases with and without clustered hosts, hosts that you upgrade on the same machine on which they are currently running (in-place upgrades), and hosts that you upgrade using different machines (migration upgrades).

This chapter includes the following topics:

Moving Virtual Machines Using vMotion During an Upgrade

This scenario is a migration upgrade. The migration upgrade is a managed transition rather than a strict upgrade. By using vMotion to move virtual machines directly from one production host to another production host, you minimize downtime of the virtual machines.

The following example provides a high-level overview of the upgrade process in an environment with ESX 4.0/ESXi 4.0 or higher and vCenter Server 5.5, using vMotion to migrate your running virtual machines to ESXi 5.5. The hosts in your environment must be licensed for and able to use vMotion.

You can perform a migration upgrade without vMotion. The only difference is the amount of downtime for the virtual machines.

A migration upgrade calls for sufficient resources to run the production environment partly on older hosts and partly on upgraded hosts. Any required redundancies and safeguards must be available on both upgraded and non-upgraded infrastructure during the transition.

Prerequisites

- Verify that one or more machines meets ESXi 5.5 requirements.
- Verify that empty host storage is sufficient to hold a portion of your production virtual machines. Ideally, the storage is large enough to hold all of the migrated virtual machines. A larger capacity for virtual machines on this extra storage means fewer operations are required before all your virtual machines are migrated.
- If your environment has vCenter Guided Consolidation, uninstall it.
- Run the Host Agent Pre-Upgrade Checker. See "Run the vCenter Host Agent Pre-Upgrade Checker," on page 57.

- Upgrade vCenter Server version 5.5. See Chapter 4, "Upgrading vCenter Server," on page 61.

  The downtime required for this upgrade is based on the amount of data in the database. During this time, you cannot perform provisioning operations, such as cloning or creating virtual machines.

- Install the version 5.5 vSphere Web Client. See "Install or Upgrade the vSphere Web Client," on page 128.

- If your environment has vSphere Update Manager, upgrade it to the latest version. See Chapter 6, "Upgrading Update Manager," on page 139.

Procedure

1 Use vMotion to move the virtual machines from the ESX 4.0/ESXi 4.0 or higher host.

2 Upgrade the host to ESXi 5.5, or perform a fresh installation of ESXi 5.5.

3 Add the ESXi 5.5 host to vCenter Server.

4 Use vMotion to move the virtual machines that you removed from the ESX 4.0/ESXi 4.0 or higher host before the upgrade.

  For vMotion to work, the hosts must be managed by the same vCenter Server instance.

What to do next

For all hosts and virtual machines in the migration upgrade, take the following actions.

- Upgrade your virtual machines. See Chapter 8, "Upgrading Virtual Machines and VMware Tools," on page 215.

- Upgrade your product licenses:

  a Get your new license keys by email, or by using the license portal.

  b Apply the new license keys to your assets using the vSphere Web Client).

- Use the vSphere Web Client to upgrade the host datastore to VMFS5.

  See the information about upgrading datastores to VMFS5 in the *vSphere Storage* documentation.

Moving Powered Off or Suspended Virtual Machines During an Upgrade with vCenter Server

In a cold migration upgrade, you power off or suspend the virtual machines that you move to a new host. When you use cold migration to move virtual machines, more downtime is required for the virtual machines.

This scenario assumes that the hosts do not have vMotion capabilities.

Upgrades using cold migrations are useful for situations that require a multistep upgrade, such as upgrades from versions lower than ESX 4.x.

Prerequisites

- Verify that one or more machines meets ESXi 5.5 requirements.

- Verify that empty host storage is sufficient to hold a portion of your production virtual machines. Ideally, the storage is large enough to hold all of the migrated virtual machines. A larger capacity for virtual machines on this extra storage means fewer operations are required before all your virtual machines are migrated.

- If your environment has vCenter Guided Consolidation, uninstall it before upgrading.

- Run the Host Agent Pre-Upgrade Checker. See "Run the vCenter Host Agent Pre-Upgrade Checker," on page 57.

- Upgrade vCenter Server to version 5.5. See Chapter 4, "Upgrading vCenter Server," on page 61.
- Install the version 5.5 vSphere Web Client. See "Install or Upgrade the vSphere Web Client," on page 128.
- If your environment has vCenter Update Manager, upgrade it to the latest version.

Procedure

1 Add the ESXi 5.5 host to vCenter Server 5.5.

2 Add the ESX 4.x/ESXi 4.x hosts to vCenter Server 5.5.

3 Power off or suspend the virtual machines on the ESX 4.x/ESXi 4.x hosts.

4 Move the virtual machines to the ESXi 5.5 host.

What to do next

For all hosts and virtual machines in the migration upgrade, take the following actions.

- Upgrade your virtual machines. See Chapter 8, "Upgrading Virtual Machines and VMware Tools," on page 215.
- Upgrade your product licenses:
  a Get your new license keys by email, or by using the license portal.
  b Apply the new license keys to your assets using the vSphere Web Client.

Migrating ESX 4.x or ESXi 4.x Hosts to ESXi 5.5 in a PXE-Booted Auto Deploy Installation

This high-level overview describes the process for migrating an ESX/ESXi 4.x host to an ESXi 5.5 installation that is deployed by using vSphere Auto Deploy.

This scenario assumes the following details about your vSphere environment.

- The hosts that you are migrating are managed by a vCenter Server running vCenter Server 4.x.
- All hosts managed by that vCenter Server are running ESX/ESXi 4.x.

The following tasks provide an overview of the migration process.

1 Create host profiles for the ESXi 4.x hosts to be migrated and attach the host profiles to the hosts.

  See the *vSphere Host Profiles* documentation.

2 Upgrade the 4.x vCenter Server to version 5.5.

  See Chapter 4, "Upgrading vCenter Server," on page 61.

3 Prepare your Auto Deploy server and environment.

  This preparation includes setting up the DHCP and TFTP servers that are used to PXE-boot Auto Deploy host machines and installing VMware PowerCLI.

  See the information about preparing for vSphere Auto Deploy in the *vSphere Installation and Setup* documentation.

4 Apply an image profile for an ESXI 5.5 host that is deployed by using the Auto Deploy PowerCLI commands.

  See the information about Auto Deploy in the *vSphere Installation and Setup* documentation.

5 Use vSphere vMotion to evacuate all virtual machines from the hosts to be migrated, and place the hosts in maintenance mode.

  See the *vCenter Server and Host Management* documentation.

6 Reboot the hosts, enter the BIOS, and reconfigure the hosts to boot from the network.

   See the information about Auto Deploy in the *vSphere Installation and Setup*. For ESXi 4.x hosts with compatible host profiles, the host configuration will be restored.

7 When one host is booted, complete any host configuration that was not migrated and take a host profile from the host.

   See the *vSphere Host Profiles* documentation.

8 Clone the host profile and attach the profile to the other migrated hosts.

   See the *vSphere Host Profiles* documentation.

9 Update the answer file of each cloned profile to provide host-specific configuration details, such as the IP configuration.

   See the *vSphere Host Profiles* documentation.

Upgrading vSphere Components Separately in a Horizon View Environment

If you upgrade vSphere components separately from Horizon View components, you must back up some Horizon View data and reinstall some Horizon View software.

Instead of performing an integrated upgrade of Horizon View and vSphere components, you can choose to first upgrade all Horizon View components and then upgrade vSphere components, or the reverse. You might also upgrade only vSphere components when a new version or update of vSphere is released.

When you upgrade vSphere components separately from Horizon View components, you must perform the following additional tasks:

1 Before you upgrade vCenter Server, back up the vCenter Server database and the View Composer database.

2 Before you upgrade vCenter Server, back up the View LDAP database from a View Connection Server instance by using the `vdmexport.exe` utility.

   For instructions, see the *VMware Horizon View Administration* document. If you have multiple instances of View Connection Server in a replicated group, you need to export the data from only one instance.

3 If you use View Composer, after you upgrade all ESX/ESXi hosts that are managed by a particular vCenter Server instance, restart the View Composer service on that host.

4 After you upgrade VMware Tools in virtual machines that are used as remote desktops, reinstall View Agent.

   Reinstalling View Agent guarantees that the drivers in the virtual machine remain compatible with the other Horizon View components.

   Step-by-step instructions for running the View Agent installer appear in *Setting Up Desktop and Application Pools in VMware Horizon View*.

Index

S

T

U

V

W